Dell Data Protection | Enterprise Edition

Enterprise Server
Installation and Migration Guide

© 2014 Dell Inc.

Registered trademarks and trademarks used in the DDP|E, DDP|ST, and DDP|CE suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen Tec® and Eikon® are registered trademarks of Authen Tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. Dropbox℠ is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube®, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, Aperture®, App Store℠, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®℠, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari®, and Siri® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. GO ID®, RSA®, and SecurID® are registered trademarks of EMC Corporation. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. InstallShield® is a registered trademark of Flexera Software in the United States, China, European Community, Hong Kong, Japan, Taiwan, and United Kingdom. Micron® and RealSSD® are registered trademarks of Micron Technology, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. SAMSUNG™ is a trademark of SAMSUNG in the United States or other countries. Seagate® is a registered trademark of Seagate Technology LLC in the United States and/or other countries. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc.

This product uses parts of the 7-Zip program. The source code can be found at www.7-zip.org. Licensing is under the GNU LGPL license + unRAR restrictions (www.7-zip.org/license.txt).

2014-11

Protected by one or more U.S. Patents, including: Number 7665125; Number 7437752; and Number 7665118.

Information in this document is subject to change without notice.

Contents

1 Getting Started with Dell Data Protection 5

Implementation Phases 5

Kick-off and Requirements Review 5

Preparation Checklist - Initial Implementation 7

Preparation Checklist - Upgrade/Migration 9

2 Introduction 13

About Dell Enterprise Server 13

Customer Support 13

3 Requirements and Architecture 15

Requirements 15

Dell Enterprise Server Prerequisites 15

Dell Enterprise Server Hardware 16

Dell Enterprise Server Software 16

Architecture Design 18

Up to 5,000 Endpoints 18

5,000 - 20,000 Endpoints 19

20,000 - 40,000 Endpoints 20

40,000 - 60,000 Endpoints 21

High Availability Considerations 22

Virtualization 23

4 Pre-Installation Configuration 25

5 Install or Upgrade/Migrate 33

New Installation 33

Main Server(s) 33

Front End Server(s) 35

Upgrade/Migration 36

Main Server(s) 37
Front End Server(s) 39

6 Post-Installation Configuration 41

EAS Management Installation and Configuration 41

Dell Security Server in DMZ Mode Configuration 43

APNs Enrollment 44

Use Windows Authentication 45

Use the Dell Server Configuration Tool 46

7 Web Browser Version of Silverlight Console Configuration 59

8 Administrative Tasks 65

Assign Dell Administrator Role 65

Log in with Dell Administrator Role 65

Upload Client Access License 65

Apply a Policy Template 65

Commit Policies 66

Configure Dell Compliance Reporter 66

Perform Back-ups 67

9 Troubleshooting 69

Appendix A 71

Appendix B 73

Appendix C 75

Getting Started with Dell Data Protection

Implementation Phases

The basic implementation process includes these phases:

- Perform Kick-off and Requirements Review
- Complete Preparation Checklist - Initial Implementation or Preparation Checklist - Upgrade/Migration
- Install or Upgrade/Migrate Dell Enterprise Server

  For instructions about client requirements and software installation, see *Enterprise Edition Administrator Guide*, *Personal Edition Installation Guide*, *Security Tools Installation Guide*, or *Enterprise Edition for Mac Administrator Guide.*
- Configure Initial Policy (see Administrative Tasks)
- Execute Test Plan
- Client Packaging
- Participate in Dell Data Protection Administrator basic knowledge transfer
- Implement Best Practices
- Coordinate Pilot or Deployment Support with Dell Client Services

Kick-off and Requirements Review

Before installation, it is important to understand your environment and the business and technical objectives of your project, to successfully implement Dell Data Protection | Encryption to meet these objectives. Ensure that you have a thorough understanding of your organization's overall data security requirements.

The following are some common key questions to help the Dell Client Services Team understand your environment and requirements:

1. What is your organization's type of business (health care, etc)?
2. What regulatory compliance requirements do you have (HIPAA/HITECH, PCI, etc.)?
3. What is the size of your organization (number of users, number of physical locations, etc.)?
4. What is the targeted number of endpoints for the deployment? Are there plans to expand beyond this number in the future?
5. Do end users have "local admin" privileges?
6. What data and devices do you need to manage and encrypt (local fixed disks, USB, etc.)?
7. What products are you considering deploying?
   - Enterprise Edition (Windows clients)
   - Enterprise Edition (SED clients)
   - Authentication
   - BitLocker Manager
   - Cloud Edition
   - External Media Shield (EMS)
   - Enterprise Edition (Mac clients)
   - Mobile Edition for Android, iOS, and Windows Phone
8. What type of user connectivity does your organization support? Types might include the following:
   - Local LAN connectivity only
   - VPN-based and/or enterprise wireless users
   - Remote/disconnected users (users not connected to the network either directly or via VPN for extended periods of time)
   - Non-domain workstations
9. What data do you need to protect at the endpoint? What type of data do typical users have at the endpoint?

10 What user applications may contain sensitive information? What are the application file types?

11 How many domains do you have in your environment? How many are in-scope for encryption?

12 What Operating Systems and OS versions are targeted for encryption?

   For a list of Operating Systems supported with Dell Data Protection | Encryption, see *Enterprise Edition Administrator Guide*, *Personal Edition Installation Guide*, *Security Tools Installation Guide*, or *Enterprise Edition for Mac Administrator Guide*.

13 Do you have alternate boot partitions configured on your endpoints?

   a Manufacturer Recovery Partition

   b Dual-boot Workstations

Preparation Checklist - Initial Implementation

Use the following checklist to ensure you've met all prerequisites before beginning to install Dell Data Protection I Encryption (DDPIE).

Proof of Concept environment cleanup is complete (If Applicable)?

- ☐ The Proof of Concept database and application have been backed up and uninstalled (if using the same server) before the installation engagement with Dell.
- ☐ Any production endpoints used during Proof of Concept testing have been decrypted or key bundles downloaded.

NOTE: All new implementations must begin with a new database and installation of the DDPIE software. Dell Client Services will not perform a new implementation using a POC environment. Any endpoints encrypted during a Proof of Concept will need to be either decrypted or rebuilt prior to the installation engagement with Dell.

Servers meet required software specifications?

- ☐ Windows Server 2008/2012 64-bit R2 (Standard or Enterprise) is installed.
- ☐ .NET Framework 3.5 SP1 is installed.
- ☐ .NET Framework 4.0 (4.5 for Windows Server 2012) is installed.
- ☐ Windows Identity Foundation is installed.
- ☐ Windows Firewall is disabled or configured to allow (inbound) ports 80, 1099, 8000, 8050, 8084, 8443, 8445, 8888, 9000, 9011, 61613, 61616.
- ☐ Connectivity is available between Dell Enterprise Server and Active Directory (AD) over ports 88, 135, 389, 636, 3268, 3269, 49125+ (RPC) (inbound to AD).
- ☐ UAC is disabled (see Windows Control Panel – User Accounts).
- ☐ IIS Web Server Role with ASP.NET Feature is installed.

Service accounts successfully created?

- ☐ Read-only access to AD (LDAP) - basic user/domain user account is sufficient.
- ☐ If using Windows Authentication for the database, this account must also be "db_owner" on database.
- ☐ Service account must have local administrator rights to the Dell Data Protection application servers.

Software is downloaded from Dell Data Protection file transfer site (CFT)?

- ☐ Software is located at https://ddpe.credant.com or https://cft.credant.com under the "SoftwareDownloads" folder.
- ☐ If you have purchased DDPIE "on-the-box," the software can be downloaded from www.dell.com. "On-the-box" refers to software that is included with the factory computer image from Dell. DDPIE can be preinstalled at the factory on any Dell computer.

Installation key and license file are available?

- ☐ The license key is included in the original email with CFT credentials - see Example Customer Notification Email.
- ☐ The license file is an XML file located on the CFT site under the "Client Licenses" folder.

NOTE: If you purchased your licenses "on-the-box," no license file is necessary. The entitlement will be automatically downloaded from Dell upon activation of any new DDPIE client.

Database is created?

- ☐ A new database is created on a supported server - see Requirements and Architecture.
- ☐ The target database user has been given "db_owner" rights.

DNS alias created for Dell Enterprise Server and/or Policy Proxies?

It is recommended that you create DNS Aliases, for scalability. This will allow you to add additional servers later or separate components of the application without requiring client update.

- ☐ DNS aliases are created, if desired. Suggested DNS aliases:
  - Enterprise Server: ddpe-es.<domain.com>
  - Front-End Server: ddpe-fe.<domain.com>

NOTE: Split-DNS allows you use to use the same DNS name for both internal and external Front-End Services and is necessary, in some cases. Split-DNS enables you to use a single address for your clients and provides flexibility when performing upgrades or scaling the solution later. A suggested CNAME for Front-End Servers when using Split-DNS is this: ddpe-fe.<domain.com>.

Plan for SSL Certificates?

- ☐ We have an internal Certificate Authority (CA) that can be used to sign certificates and is trusted by all workstations in the environment ***or*** we plan to purchase a signed certificate using a public Certificate Authority, such as VeriSign or Entrust. If using a public Certificate Authority, please inform the Dell Client Services Engineer.

Change Control requirements identified and communicated to Dell?

- ☐ Submit any specific Change Control requirements for the installation of DDPIE to Dell Client Services prior to the installation engagement. These requirements may include changes to the application server(s), database, and client workstations.

Test Hardware prepared?

- ☐ Prepare at least three computers with your corporate computer image to be used for testing. Dell recommends that you ***not*** use live systems for testing. Live systems should be used during a production pilot after encryption policies have been defined and tested using the Test Plan provided by Dell.

Preparation Checklist - Upgrade/Migration

Use the following checklist to ensure you've met all prerequisites before beginning to upgrade Dell Data Protection I Encryption (DDPIE).

Servers meet required software specifications?

- ☐ Windows Server 2008/2012 64-bit R2 (Standard or Enterprise) is installed.
- ☐ .NET Framework 3.5 SP1 is installed.
- ☐ .NET Framework 4.0 (4.5 for Windows Server 2012) is installed.
- ☐ Windows Identity Foundation is installed.
- ☐ Windows Firewall is disabled or configured to allow (inbound) ports 80, 1099, 8000, 8050, 8084, 8443, 8445, 8888, 9000, 9011, 61613, 61616.
- ☐ Connectivity is available between Dell Enterprise Server and Active Directory (AD) over ports 88, 135, 389, 636, 3268, 3269, 49125+ (RPC) (inbound to AD).
- ☐ UAC is disabled (see Windows Control Panel – User Accounts).
- ☐ IIS Web Server Role with ASP.NET Feature is installed.

Service accounts successfully created?

- ☐ Active Directory or SQL service accounts currently used for CMG/DDPIE are identified, and the account user name(s) and password(s) are available.
- ☐ If using Windows Authentication for the database, this account must also be "db_owner" on the CMG/DDPIE database.
- ☐ Service account must have local administrator rights to the Dell Data Protection application servers.

Software is downloaded from Dell Data Protection file transfer site (CFT)?

- ☐ Software is located at https://ddpe.credant.com or https://cft.credant.com under the "SoftwareDownloads" folder.
- ☐ If you have purchased DDPIE "on-the-box," the software can be downloaded from www.dell.com. "On-the-box" refers to software that is included with the factory computer image from Dell. DDPIE can be preinstalled at the factory on any Dell computer.

Installation key and license file are available?

- ☐ The license key is included in the original email with CFT credentials - see Example Customer Notification Email.
- ☐ The license file is an XML file located on the CFT site under the "Client Licenses" folder.

NOTE: If you purchased your licenses "on-the-box," no license file is necessary. The entitlement will be automatically downloaded from Dell upon activation of any new DDPIE client.

Have enough endpoint licenses?

Prior to upgrading, please ensure that you have enough client licenses to cover all of the endpoints in your environment. If your installations currently exceed your license count, please contact your Dell Sales Representative prior to upgrading or migrating. DDPE 8.x will perform license validation, and activations will be prevented if no licenses are available.

- ☐ I have enough licenses to cover my environment.

Plan for SSL Certificates?

- ☐ We have an internal Certificate Authority (CA) that can be used to sign certificates and is trusted by all workstations in the environment ***or*** we plan to purchase a signed certificate using a public Certificate Authority, such as VeriSign or Entrust. If using a public Certificate Authority, please inform the Dell Client Services Engineer.

Change Control requirements identified and communicated to Dell?

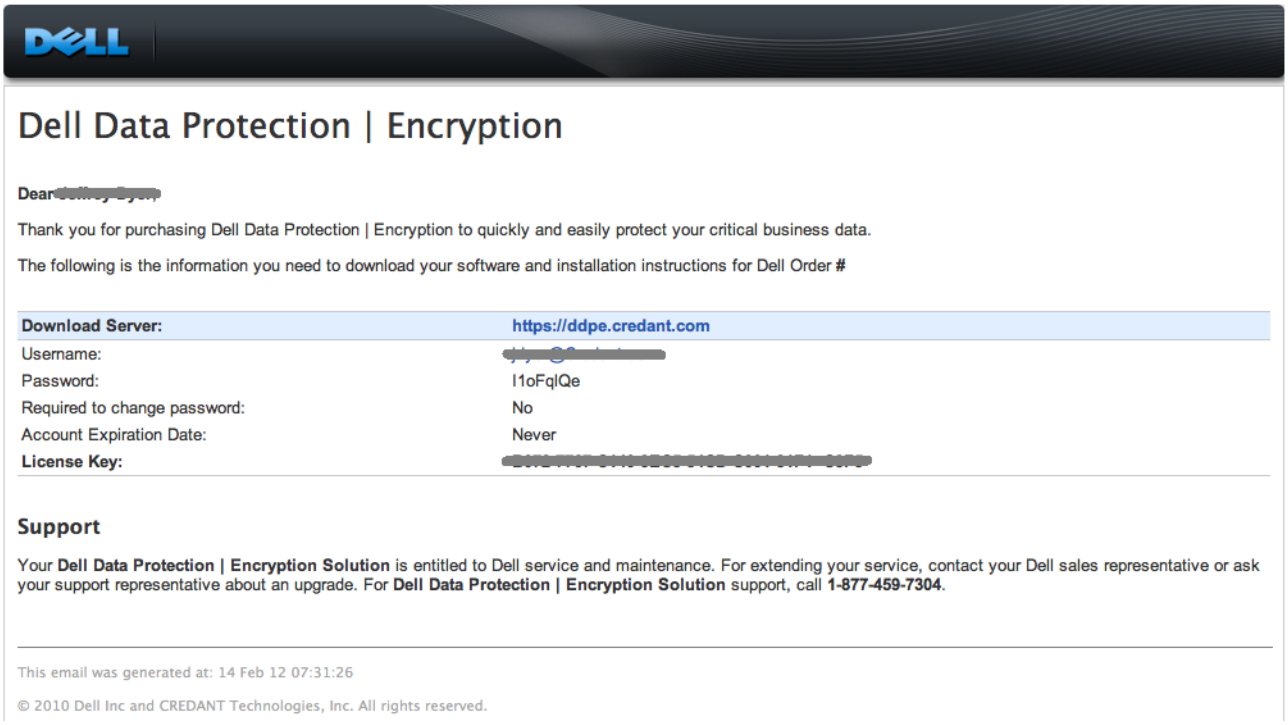
- ☐ Submit any specific Change Control requirements for the installation of DDPIE to Dell Client Services prior to the installation engagement. These requirements may include changes to the application server(s), database, and client workstations.

Test Hardware prepared?

- ☐ Prepare at least three computers with your corporate computer image to be used for testing. Dell recommends that you ***not*** use live systems for testing. Live systems should be used during a production pilot after encryption policies have been defined and tested using the Test Plan provided by Dell.

Example Customer Notification Email

After you purchase Dell Data Protection, you will receive an email from DellDataProtectionEncryption@Dell.com. Below is an example of the email, which will include your CFT credentials and License Key information.



Dell Data Protection | Encryption

Dear [redacted]

Thank you for purchasing Dell Data Protection | Encryption to quickly and easily protect your critical business data.

The following is the information you need to download your software and installation instructions for Dell Order #

Download Server:	**https://ddpe.credant.com**
Username:	[redacted]
Password:	I1oFqlQe
Required to change password:	No
Account Expiration Date:	Never
License Key:	[redacted]

Support

Your **Dell Data Protection | Encryption Solution** is entitled to Dell service and maintenance. For extending your service, contact your Dell sales representative or ask your support representative about an upgrade. For **Dell Data Protection | Encryption Solution** support, call **1-877-459-7304**.

This email was generated at: 14 Feb 12 07:31:26

© 2010 Dell Inc and CREDANT Technologies, Inc. All rights reserved.

1

Introduction

About Dell Enterprise Server

The Enterprise Server is the security administration piece of Dell's solution. The Remote Management Console allows administrators to monitor the state of endpoints, policy enforcement, and protection across the enterprise.

The Enterprise Server has the following features:

- Centralized management of devices
- Role-based security policy creation and management
- Administrator-assisted device recovery
- Separation of administrative duties
- Automatic distribution of security policies
- Trusted paths for communication between components
- Unique encryption key generation and automatic secure key escrow
- Centralized compliance auditing and reporting

Customer Support

Refer to your Welcome Letter for Dell Pro Support contact information.

When contacting Dell Pro Support, have the following information available:

- Version information for the relevant components:
  - Operating system version for the server/workstation where the components are running.
  - For the Dell Enterprise Server, the version number and build date can be found in the *About* link in the Dell Remote Management Console.
  - For the Exchange ActiveSync component (installed on the front-end Exchange Server), locate the version number from Windows Explorer. Right-click <Exchange ActiveSync install dir>\OTASyncControl.dll, select Properties, and click the *Version* tab.
- A detailed description of the issue you are experiencing.
- Information about where we can reach you.

2

Requirements and Architecture

This section details hardware and software requirements and architecture design recommendations for Dell Data Protection I Encryption implementation.

Requirements

The Dell Enterprise Server components have hardware and software requirements in addition to the software provided on the Dell installation media. Ensure that the installation environment meets the requirements before continuing with installation or upgrade/migration tasks.

Dell Enterprise Server Prerequisites

The following table details the software that must be in place before installing the Dell Enterprise Server. Links and directions to install these prerequisites are detailed in Pre-Installation Configuration.

Prerequisites
· Windows Installer 3.1 or later Windows Installer 3.1 or later must be installed on the server where the installation is taking place.
· Microsoft Visual C++ 2010 Redistributable Package If not installed, the installer will install it for you.
· Microsoft .NET Framework Version 3.5 SP1
· Microsoft .NET Framework Version 4.0 Microsoft has published security updates for .NET Framework Version 4.
· Microsoft Windows Identity Foundation
· Internet Information Services (IIS)
· Windows Server 2003 Support Tools (SP1 or SP2, depending on server version) If using Windows Server 2003
· Silverlight If you intend to use the web browser version of the Silverlight Console

Dell Enterprise Server Hardware

The following table details the *minimum* hardware requirements for Dell Enterprise Server. See Architecture Design for additional information about scaling based on the size of your organization.

NOTE: Registry locations for Dell Policy Proxy (if installed):
32-bit: HKLM\Software\CREDANT 64-bit: HKLM\Software\Wow6432Node\CREDANT

NOTE: When Enterprise Server is running on a 32-bit operating system, to access more than 4 GB physical memory, enable Physical Address Extension. For more information, see http://msdn.microsoft.com/en-us/library/windows/desktop/aa366796%28v=vs.85%29.aspx.

Dell Enterprise Server (Back-end Server)	Proxy Server (Front-end Server)
Processor	
2 GHz Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium, or AMD equivalent	Intel Pentium-class or AMD processor
RAM	
8GB minimum, depending on configuration	1 GB
Free Disk Space	
+-1.5 GB free disk space (plus virtual paging space)	+-104 MB (plus virtual paging space)
Network Card	
10/100/1000 network interface card	
Miscellaneous	
TCP/IPv4 installed and activated	

Dell Enterprise Server Software

The following table details the software requirements for the Dell Enterprise Server and Proxy Server.

NOTE: Always disable UAC when using Windows Server 2008. After disabling UAC, the server must be rebooted for this change to take effect.

Registry location for Windows Servers: HKLM\SOFTWARE\Dell.

Dell Enterprise Server (Back-end Server)	Proxy Server (Front-end Server)
Operating System	
· Windows Server 2003 SP2 - Standard Edition - Enterprise Edition	· Windows XP Professional SP3
· Windows Server 2003 R2 and R2 SP2 - Standard Edition - Enterprise Edition	· Windows 7 SP0-SP1 - Enterprise - Professional - Ultimate
· Windows Server 2008 R2 SP0-SP1 64-bit - Standard Edition - Enterprise Edition	· Windows Server 2003 SP2 - Standard Edition - Enterprise Edition
· Windows Server 2008 SP2 32-bit - Standard Edition - Enterprise Edition	· Windows Server 2003 R2 and R2 SP2 - Standard Edition - Enterprise Edition

· Windows Server 2008 SP2 64-bit - Standard Edition - Enterprise Edition	· Windows Server 2008 R2 SP0-SP1 64-bit - Standard Edition - Enterprise Edition
· Windows Server 2012 R2 - Standard	· Windows Server 2008 SP2 32-bit - Standard Edition - Enterprise Edition
	· Windows Server 2008 SP2 64-bit - Standard Edition - Enterprise Edition
	· Windows Server 2012 R2 - Standard

Exchange ActiveSync Servers

If you intend to use Dell Data Protection | Mobile Edition, the following Exchange ActiveSync Servers are supported. This component is installed on your front-end Exchange Server.

· Exchange ActiveSync 12.0 – a component of Exchange Server 2007

· Exchange ActiveSync 12.1 – a component of Exchange Server 2007 SP1

· Exchange ActiveSync 14.0 – a component of Exchange Server 2010

· Exchange ActiveSync 14.1 – a component of Exchange Server 2010 SP1

Microsoft Message Queuing (MSMQ) must be installed/configured on the Exchange Server.

LDAP Repository

· Microsoft Active Directory 2003

· Microsoft Active Directory 2008

Recommended Virtual Environments for Dell Enterprise Server Components

The Dell Enterprise Server can optionally be installed in a virtual environment. Only certain environments are recommended and there may be performance considerations as described below.

· Dell Enterprise Server v8.5 has been validated with VMWare ESX/ESXi 5.5.

NOTE: When running VMWare ESX/ESXi and Windows Server 2012 R2, VMXNET3 Ethernet Adapters are recommended.

· Microsoft Windows Server 2008 R2 Hyper-V

Dell Enterprise Server Performance in a Virtual Environment

· Dell has observed up to a 50% performance impact, depending on environment. The impact is most noticeable during activation, inventory processing, and triage. If performance is a concern, we recommend deploying to a non-virtual server environment.

· The Microsoft SQL Server database hosting the Dell Enterprise Server should be run on a separate computer and on real hardware.

Database

· Microsoft SQL Server 2005 SP1, SP2, and SP3 Standard Edition / Enterprise Edition

· Microsoft SQL Server 2008 and Microsoft SQL Server 2008 R2 Standard Edition / Enterprise Edition

· Microsoft SQL Server 2012 Standard Edition / Business Intelligence / Enterprise Edition

NOTE: Express Editions are not supported for production environments. Express Editions may be used in POC and evaluations only.

Web Browsers

Silverlight Console

· Internet Explorer 7.x or later

Dell Compliance Reporter

· Internet Explorer 7.x or later

· Mozilla Firefox 2.x or later

· Google Chrome

Architecture Design

The Dell Data Protection | Encryption solution is a highly scalable product, scaled on the size of your organization and the number of endpoints targeted for encryption. This section provides a set of guidelines for scaling the architecture for 5,000 to 60,000 endpoints.

NOTE: If the organization has more than 50,000 endpoints, please contact Dell Client Services for assistance.

NOTE: Each of the components listed in each section include the minimum hardware specifications, which are required to ensure optimal performance in most environments. Failing to allocate adequate resources to any of these components may result in performance degradation or functional problems with the application.

Up to 5,000 Endpoints

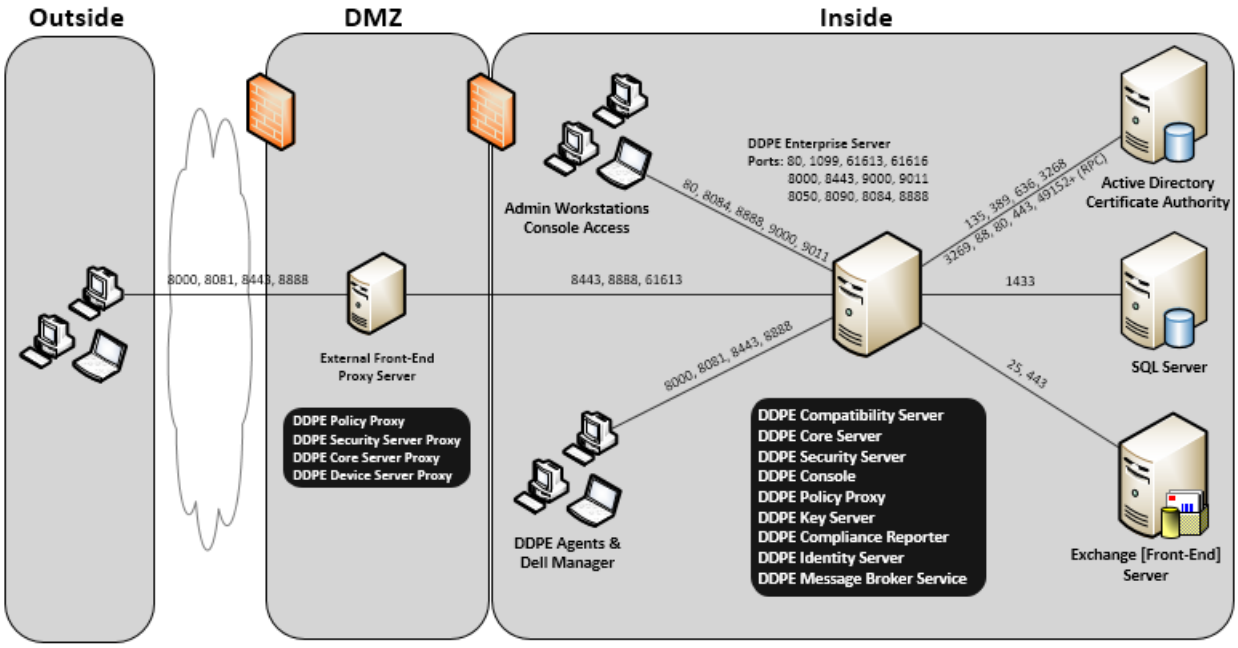
This architecture accommodates most small to medium size businesses ranging between 1 and 5,000 endpoints. All DDPE server components can be installed on a single server. Optionally, a front-end server can be placed in the DMZ for publishing policies and/or activating endpoints over the Internet.

Architecture Components

Dell Enterprise Server

Dell External Front-End Server

SQL Server



5,000 - 20,000 Endpoints

This architecture accommodates environments ranging between 5,000 and 20,000 endpoints. A front-end server is added to distribute the additional load and is designed to handle approximately 15,000 - 20,000 endpoints. Optionally, a front-end server can be placed in the DMZ for publishing policies and/or activating endpoints over the Internet.

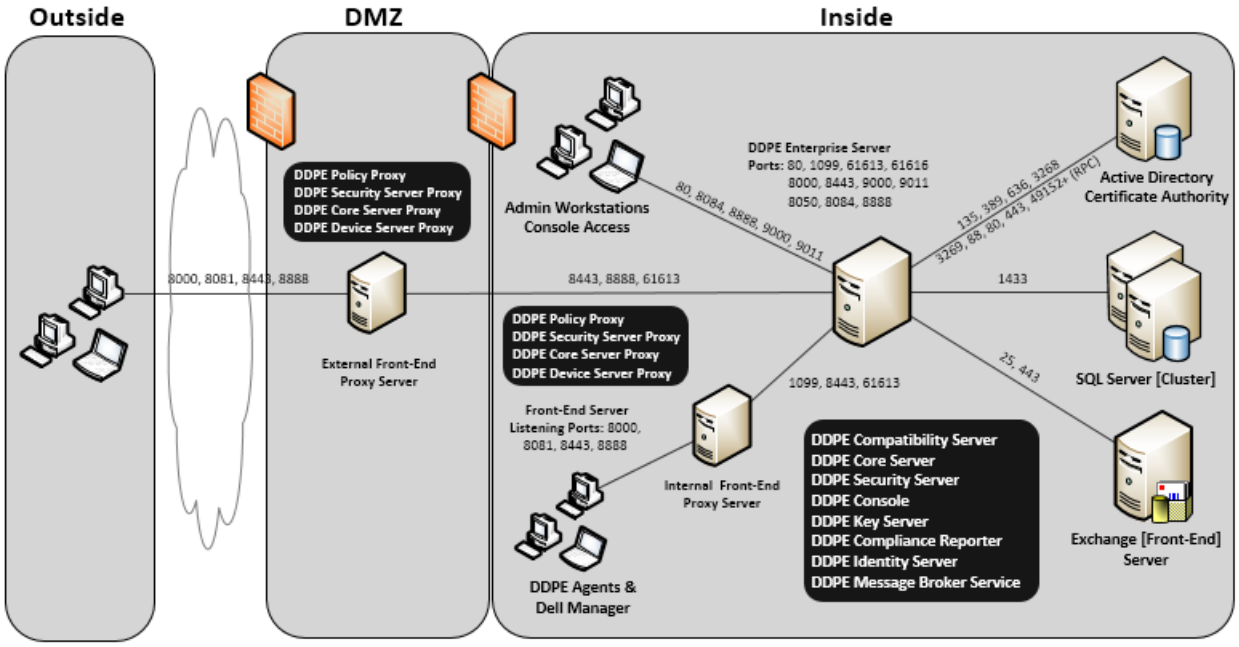
Architecture Components

Dell Enterprise Server

Dell Internal Front-End Server

Dell External Front-End Server

SQL Server



20,000 - 40,000 Endpoints

This architecture accommodates environments ranging between 20,000 and 40,000 endpoints. An additional front-end server is added to distribute the additional load. Each front-end server is designed to handle approximately 15,000 - 20,000 endpoints. Optionally, a front-end server can be placed in the DMZ for activating endpoints and/or publishing policies to endpoints over the Internet.

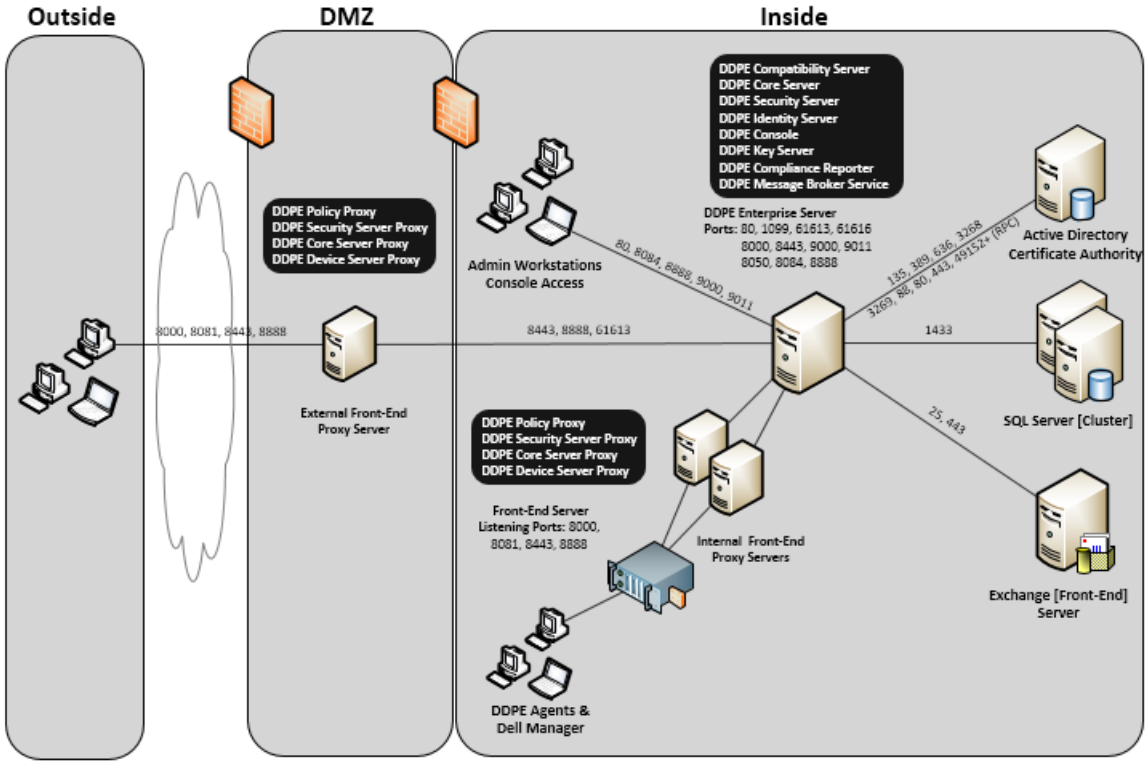
Architecture Components

Dell Enterprise Server

Dell Internal Front-End Servers (2)

Dell External Front-End Server

SQL Server



40,000 - 60,000 Endpoints

This architecture accommodates environments ranging between 40,000 and 60,000 endpoints. An additional front-end server is added to distribute the additional load. Each front-end server is designed to handle approximately 15,000 - 20,000 endpoints. Optionally, a front-end server can be placed in the DMZ for activating endpoints and/or publishing policies to endpoints over the Internet.

NOTE: If the organization has more than 50,000 endpoints, please contact Dell Client Services for assistance.

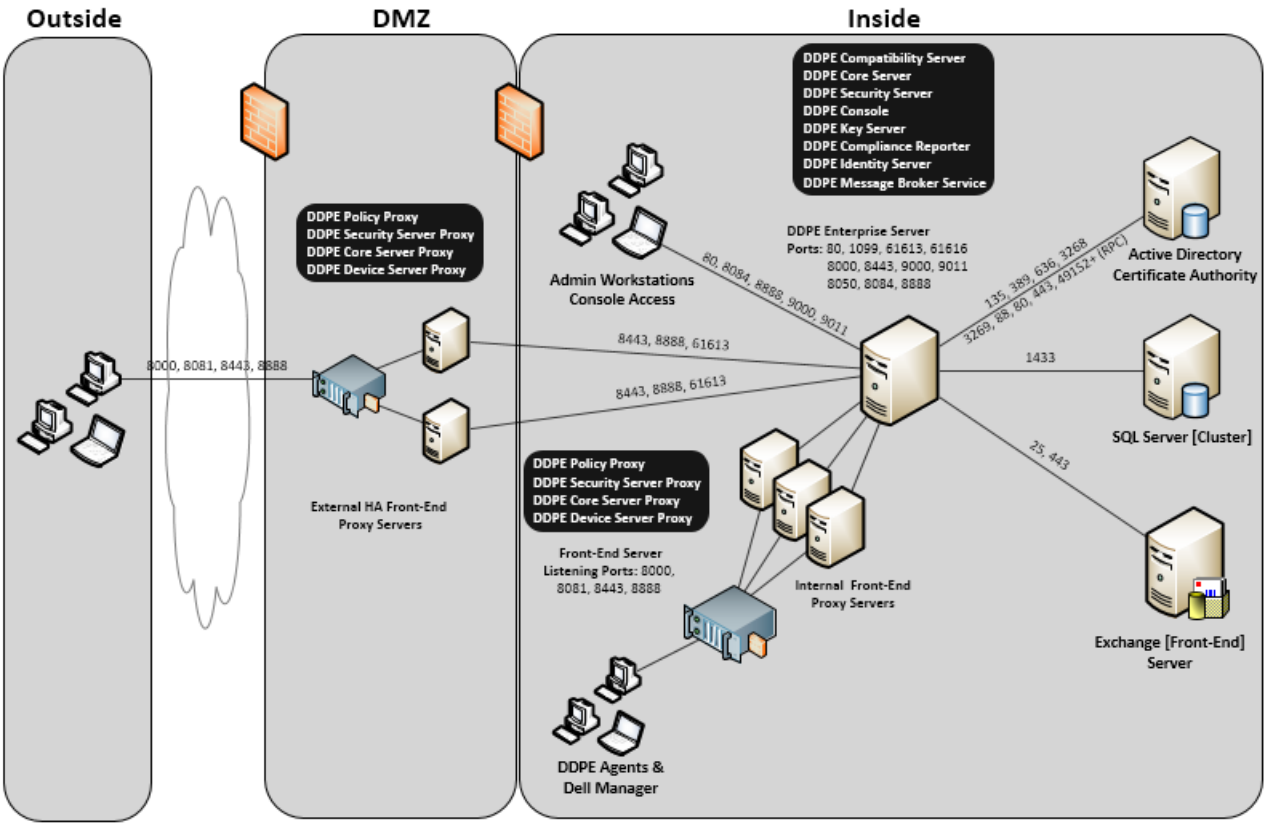
Architecture Components

Dell Enterprise Server

Dell Internal Front-End Servers (2)

Dell External Front-End Server

SQL Server



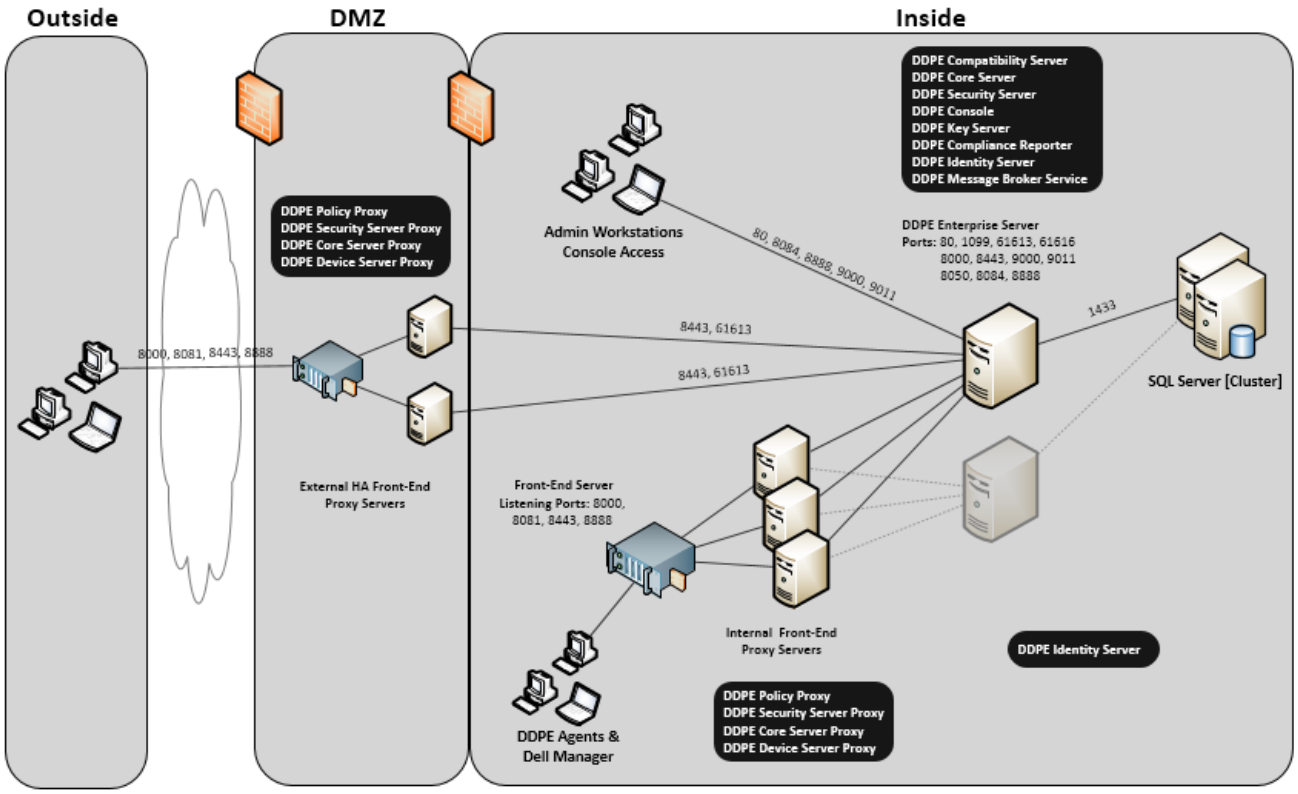
High Availability Considerations

This architecture depicts a highly available architecture supporting up to 60,000 endpoints. There are two Dell Enterprise Servers set up in an active/passive configuration. To failover to the second Dell Enterprise Server, stop the services on the primary node and point the DNS Alias (CNAME) to the second node. Start the services on the second node and launch the console to ensure the application is working properly. Services on the second (passive) node should be configured as "Manual" in order to prevent those services from accidentally starting during regular maintenance and patching.

An organization can also choose to have an SQL Cluster database server. In this configuration, the Dell Enterprise Server should be configured to use the cluster IP or hostname.

NOTE: Database replication is not supported.

Client traffic is distributed across three internal front-end servers. Optionally, multiple front-end servers can also be placed in the DMZ for activating endpoints and/or publishing policies to endpoints over the Internet.



Virtualization

Dell Data Protection Application Servers

Disk speed on the hardware that hosts the virtual server, RAM allocation to the guest, and storage configuration may cause significant performance impact. The impact is most noticeable during activation, policy and inventory processing, and triage. Dell recommends reserving as much RAM as possible for the virtual host, and giving the virtual host priority in resource allocation. If performance is a concern, Dell recommends deploying to a non-virtual server environment.

SQL Server

In larger environments, it is highly recommended that the SQL Database server run on physical hardware and on a redundant system, such as a SQL Cluster, to ensure availability and data continuity. It is also recommended to perform daily full backups with transactional logging enabled to ensure that any newly generated keys through user/device activation are recoverable.

Database maintenance tasks should include rebuilding of all databases indexes and collecting statistics.

For additional information on SQL Server best practices, please see SQL Server Best Practices.

3

Pre-Installation Configuration

Before you begin, read the Release Notes for any current workarounds or known issues related to Dell Enterprise Server.

The pre-installation configuration of the server(s) where you intend to install the Dell Enterprise Server is very important. Pay special attention to this section to ensure a smooth installation of the Dell Enterprise Server.

Configuration

1 If enabled, turn off User Access Control (UAC) and Internet Explorer Enhanced Security Configuration (ESC). Add the Server URL to Trusted Sites in the browser security options. Reboot the server.

2 Open the following ports for each component:

Internal:

Active Directory communication: TCP/389

Email communication (optional): 25

To Front End (if needed):

Communication from external Dell Policy Proxy to Dell Message Broker: TCP/61616 and STOMP/61613

Communication to back-end Dell Security Server: HTTPS/8443

Communication to back-end Dell Core Server: HTTPS/8888 and 9000

Communication to RMI ports - 1099

Communication to back-end Dell Device Server: HTTP(S)/8081 - If your Dell Enterprise Server is v7.7 or later. If your Dell Enterprise Server is pre-v7.7, HTTP(S)/8443

External (if needed):

SQL Database: TCP/1433

Silverlight Console: HTTP/80

LDAP: TCP/389/636 (local domain controller), TCP/3268/3269 (global catalog), TCP/135/49125+ (RPC)

Dell Compatibility Server: TCP/1099

Dell Compliance Reporter: HTTP(S)/8084

Dell Console Web Services: HTTP/9011

Dell Identity Server: HTTPS/8445

Dell Core Server: HTTPS/8888 and 9000

Dell Device Server: HTTP(S)/8081 (Dell Enterprise Server v7.7 or later) or HTTP(S)/8443 (Pre-v7.7 Dell Enterprise Server)

Dell Key Server: TCP/8050

Dell Policy Proxy: TCP/8000

Dell Security Server: HTTPS/8443

NOTE: If your Enterprise Edition clients will be entitled from the factory or you purchase licenses from the factory, set the GPO on the domain controller to enable entitlements (this may not be the server running Enterprise Edition). Ensure that outbound port 443 is available to communicate with the Server. If port 443 is blocked for any reason, the entitlement functionality will not work. For more information, see *Enterprise Edition Administrator Guide*.

Create Dell Database

3 If you do not yet have a Microsoft SQL database configured for Dell, follow the instructions below. Create the SQL database and SQL user in SQL Management Studio.

The Dell Enterprise Server is prepped for both SQL and Windows Authentication. The default authentication method is SQL Authentication. If you wish to use Windows Authentication, additional configuration steps are needed after the installation/upgrade/migration, but **before** using the Dell Server Configuration Tool. The additional steps needed are detailed in Use Windows Authentication.

Create the database and then create a Dell database user with db_owner rights. The db_owner may assign permissions, back up and restore the database, create and delete objects, and manage user accounts and roles without any restrictions. Additionally, ensure that this user has permissions/privileges to run stored procedures.

Create a New Microsoft SQL Server Database using Windows Authentication:

a Click **Start** > **All Programs** > **Microsoft SQL Server** > **Management Studio**.

b Right-click the Databases folder, and then click New Database. The Database Properties dialog displays.

c Enter the Database Name and click **OK**.

d Expand the *Security* folder, and right-click **Logins**.

e Click **New Login** to create an owner for the new database.

f Enter a username in the *Name* field.

g Select the Authentication option *Windows Authentication*.

h Select **User Mapping** and then highlight the new database.

i Select the database role (db_owner), and click **OK**.

OR

Create a New Microsoft SQL Server Database using SQL Server Authentication:

a Click **Start** > **All Programs** > **Microsoft SQL Server** > **Management Studio**.

b Right-click the *Databases* folder, and then click **New Database**. The *Database Properties* dialog displays.

c Enter the Database Name and click **OK**.

d Expand the *Security* folder, and right-click **Logins**.

e Click **New Login** to create an owner for the new database.

f Enter a username in the *Name* field.

g Select the Authentication option *SQL Server Authentication*. Enter and confirm the password.

h Deselect **Enforce Password Expiration**.

i Select **User Mapping** and then highlight the new database.

j Select the database role (db_owner), and click **OK**.

Install Windows Installer 3.1 or later

4 *If not already installed*, install Windows Installer 3.1 or later.

Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 – (***3.1***) – http://www.microsoft.com/downloads/en/details.aspx?FamilyID=889482FC-5F56-4A38-B838-DE776FD4138C&displaylang=en

Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 – (***4.5***) – http://www.microsoft.com/downloads/en/details.aspx?FamilyId=5A58B56F-60B6-4412-95B9-54D056D6F9F4&displaylang=en

Install Microsoft Visual C++ 2010 Redistributable Package

5 *If not already installed*, install Microsoft Visual C++ Redistributable Package. If desired, you can allow the Dell Enterprise Server installer to install this component.

Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 – http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5555

Install Windows Server 2003 Support Tools

6 *If using Windows Server 2003*, install Windows Server 2003 Support Tools.

Service Pack 1 32-bit
http://www.microsoft.com/downloads/en/details.aspx?FamilyId=6EC50B78-8BE1-4E81-B3BE-4E7AC4F0912D&displaylang=en

Service Pack 2 32-bit
http://www.microsoft.com/downloads/en/details.aspx?FamilyID=96a35011-fd83-419d-939b-9a772ea2df90&DisplayLang=en

Install .NET Framework 3.5.1 Features

Omit this step for Windows Server 2003. The steps for Windows Server 2008 and Windows Server 2008 R2 are essentially the same.

7 Install .NET Framework 3.5.1 Features.

a Start Server Manager.

b Select **Features**.

c Expand the *Features Summary* in the right pane and click **Add Features**.

d Select the checkbox for **.NET Framework 3.5.1 Features**. Depending on server version, this may be listed as **.NET Framework 3.0 Features**. If so, select that option.

You may be required to install .NET Framework 3.5.1 Roles Services before proceeding. If so, click **Add Required Role Services**.

e Click **Next** to begin installation of .NET Framework 3.5.1 Features.

f At the *Web Server (IIS)* window, click **Next**.

g At the *Select Role Service*s window, leave the default values as-is and click **Next**.

h At the *Confirm Installation Selections* window, click **Install**.

i Once the installation finishes, an *Installation Succeeded* message displays. Click **Close**.

Install .NET Framework 3.5 SP1

8 Install .NET Framework 3.5 SP1.

Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 – http://www.microsoft.com/downloads/en/details.aspx?familyid=AB99342F-5D1A-413D-8319-81DA479AB0D7&displaylang=en

Install .NET Framework 4.0

9 Install .NET Framework 4.0.

Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 – http://www.microsoft.com/downloads/en/details.aspx?FamilyID=9cfb2d51-5ff4-4491-b0e5-b386f32c0992&displaylang=en

Add Web Server (IIS) Role and ASP.NET Role Service

This only needs to be completed if you intend to use the web browser version of the Silverlight Console.

10 Add Web Server (IIS) Role and ASP.NET Role Service [ASP.NET Role Service is a component of the Web Server (IIS) Role].

Windows Server 2003 –
http://www.microsoft.com/TechNet/prodtechnol/WindowsServer2003/Library/IIS/750d3137-462c-491d-b6c7-5f370d7f26cd.mspx?mfr=true

Windows Server 2008 and Windows Server 2008 R2 –
http://learn.iis.net/page.aspx/29/installing-iis-7-on-windows-server-2008-or-windows-server-2008-r2/

Ensure that the following features are configured:

- Common HTTP Features - Static Content, Default Document
- Application Development - .Net Extensibility

To display the current IIS configuration, enter the following powershell command:

Import-Module ServerManager

Get-WindowsFeature > c:\iis-features.txt

The 'Get-WindowsFeature > c:\iis-features.txt' command creates a text file with the list.

To change the IIS configuration, enter the following powershell command:

Import-Module ServerManager

Add-WindowsFeature Web-Server,Web-WebServer,Web-Static-content,Web-Default-Doc,Web-Dir-Browsing,Web-Http-Errors,Web-asp-net,Web-net-ext,web-isapi-ext,web-isapi-filter,web-http-logging,web-request-monitor,web-filtering,web-stat-compression,web-mgmt-console

Windows Server 2012 R2 –
http://www.iis.net/learn/install/installing-iis-85/installing-iis-85-on-windows-server-2012-r2

Ensure that the following features are configured:

- Common HTTP Features - Static Content, Default Document
- Application Development - .Net Extensibility - Expand the hierarchy, and select ASP .NET 3.5 and 4.5

To display the current IIS configuration, enter the following powershell command:

Import-Module ServerManager

Get-WindowsFeature > c:\iis-features.txt

The 'Get-WindowsFeature > c:\iis-features.txt' command creates a text file with the list.

To change the IIS configuration, enter the following powershell command:

Import-Module ServerManager

Add-WindowsFeature Web-Server,Web-WebServer,Web-Static-content,Web-Default-Doc,Web-Dir-Browsing,Web-Http-Errors,Web-asp-net,Web-net-ext,web-isapi-ext,web-isapi-filter,web-http-logging,web-request-monitor,web-filtering,web-stat-compression,web-mgmt-console

Install Windows Identity Foundation

11 Install Windows Identity Foundation.

Windows Server 2003 – http://www.microsoft.com/downloads/en/details.aspx?FamilyID=be4db6a0-b76d-446d-810c-ea3c25b3969a&displaylang=en

Windows Server 2008 and Windows Server 2008 R2 – http://www.microsoft.com/downloads/en/details.aspx?FamilyID=eb9c345f-e830-40b8-a5fe-ae7a864c4d76&displaylang=en

Windows Server 2012 R2 - In Server Manager Add Roles and Features Wizard, select **Features** then **Windows Identity Foundation 3.5**. Click **Next**, then click **Install**.

Configure Microsoft CA (MSCEP)

This step only needs to be completed if you intend to use iOS with Dell Data Protection | Mobile Edition

12 Configure MSCEP.

Windows Server 2003:

a Install the IIS Service. Go to **Start > Control Panel > Add or Remove Programs**.

In Add or Remove Programs, click **Add/Remove Windows Components.**

Under Components, click **Application Server** (but do NOT select it) and press **Details**.

In the *Application Server* window, check the *Internet Information Services (IIS)* check box and click **OK**.

Click **Next** at the *Windows Components* window.

After the wizard completes the installation, click **Finish**.

b Install the CA Service. Click **Start > Control Panel > Add or Remove Programs**.

In Add or Remove Programs, click **Add/Remove Windows Components.**

Under Components, select **Certificate Services** and click Next.

A warning about domain membership and computer renaming constraints displays. Click **Yes** to continue.

At the *CA Type* window, select **Stand-alone root CA**, and click **Next**.

At the *CA Identifying Information* window, in the *Common name for this CA* field, enter the name of the server, and click **Next**.

At the *Certificate Database Settings* window, accept the defaults in both the *Certificate database* and *Certificate database log* fields and click **Next**.

A prompt displays to stop *Internet Information Services*. Click **Yes**.

At the prompt to *Enable Active Server Pages (ASPs)*, click **Yes**.

When the installation process is complete, click **Finish**.

c Install the Simple Certificate Enrollment Protocol (SCEP) Add-On for Certificate Services. Click **Start > Run** then enter **<drive>:cepsetup.exe** (where drive is the CD-ROM drive where the Windows Server 2003 Resource Kit CD is located or the disk drive where you have downloaded cepsetup.exe). This starts the SCEP Add-On for Certificate Services Setup wizard. Click **Yes**.

Click **Yes** to accept the license agreement for *SCEP Add-On for Certificate Services*.

Click **Next** at *Welcome* dialog.

Select **Use local system account** and click **Next**.

Deselect **Require SCEP Challenge Phrase to Enroll** and click **Next**.

A warning about disabling the challenge phrase option for enrollment displays. Click **Yes** to continue.

Click **Finish** to complete installation.

A Setup Successful message displays. **Make a note of the URL in this message; you will need it later.** Click **OK**.

Open IIS Manager. Drill into **<Server>/Web Sites/CertSrv/**.

Right-click **mscep** and select *Properties.*

Select the *Directory Security* tab and click **Edit** for Authentication and access control.

In the bottom half of the dialog, deselect *Integrated Windows authentication* and click **OK**.

From the *Administrative Tools* menu, open Certification Authority.

Right-click your Authority and select **Properties**.

Select the *Policy Module* tab and click **Properties**.

At the *Request Handling* window, select ***"Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate."*** option and click **Apply.**

d Close IIS Manager.

e Restart the server. To verify, open Internet Explorer and in the address bar, enter the URL you made a note of earlier. The format is http://server.domain.com/certsrv/mscep/mscep.dll.

End of MSCEP Windows Server 2003 setup.

Windows Server 2008 R2 (must be Enterprise Edition, *Standard Edition will not allow the MSCEP role to be installed*):

a Open Server Manager. In the left menu, select **Server Roles** and check the box for **Active Directory Certificate Services**. Click **Next**. The Add Roles Wizard advances you to the next steps.

In *AD CS > Role Services.*., check the boxes for **Certification Authority** and **Certification Authority Web Enrollment** role services. Select **Add Required Role Services for Web Server IIS** (if prompted). Click **Next**.

In *AD CS > Setup Type*, select **Standalone**. Click **Next**.

In *AD CS > CA Type*, select **Subordinate CA**. Click **Next**.

In *AD CS > Private Key*, select **Create a new private key**. Click **Next**.

In *AD CS > Private Key > Cryptography.*, keep the defaults of **RSA#Microsoft Software Key Storage Provider**, **2048** and **SHA1**. Click **Next**.

In *AD CS > Private Key > CA Name,* keep all of the default values. Click **Next**.

In *AD CS > Private Key > Certificate Request.*., select **Send a certificate request to a parent: CA**. Select **Browse by: CA name**. Browse to and select **Parent CA**. Click **Next**.

In *AD CS > Certificate Database*, keep the default values. Click **Next**.

In *Web Server (IIS)*, click **Next**.

In *Web Server (IIS) > Role Services*, keep the default values. Click **Next**.

In *Confirmation*, click **Install**.

In *Result*s, review the results and click **Close**.

In *Server Manager > Roles*, select **Add Role Services** under *Active Directory Certificate Services*.

When the *Select Role Services* window displays, check the box for **Network Device Enrollment Service**. Click **Next**.

Add the user account that *Network Device Enrollment Service* should use when authorizing certificate requests to the Users Group of IIS_IUSRS of the local server. The format is Domain\UserName. Click **OK**.

At the Specify User Account windows, select the user that was just added to the IIS_IUSRS group. Click **Next**.

At the *Specify Registration Authority Information* window, keep the default values for *Required Information* and *Add Optional Information* as desired. Click **Next**.

At the *Configure Cryptography for Registration Authority* window, keep the default values. Click **Next**.

At the *Confirm Installation Selections* window, click **Install**.

At the *Installation Results* window, review the results and click **Close**.

Close Server Manager.

b Modify Registry Key as follows:

HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword
"EnforcePassword"=dword:00000000

c Open IIS Manager. Drill into **\<ServerName>\Sites\Default Web Site\CertSrv\mscep_admin**.

Open *Authentication* and enable **Anonymous Authentication**.

d Click **Start > Run**. Type *certsrv.msc* and click **Enter**.

When the *certsrv* window displays, right-click the server name, select **Properties** and click the *Policy Module* tab.

Click **Properties** and select **Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate.** Click **OK**.

e Close IIS Manager.

f Restart the server. To verify, open Internet Explorer and in the address bar, enter http://server.domain.com/certsrv/mscep_admin/.

End of MSCEP Windows Server 2008 R2 setup.

Install/Configure Microsoft Message Queuing (MSMQ)

This step only needs to be completed if you intend to use Dell Data Protection | Mobile Edition This is a prerequisite for the EAS Device Manager and EAS Mailbox Manger to be able to communicate.

13 Install MSMQ 4.0 on Windows Server 2008 or Windows Server 2008 R2 (on the server hosting the Exchange environment) – http://msdn.microsoft.com/en-us/library/aa967729.aspx

Optional

14 **For a new installation or an upgrade/migration for 7.x/8.x** – copy your Product Key (the name of the file is *EnterpriseServerInstallKey.ini*) to **C:\Windows** to automatically populate the 32-character Product Key in the Dell Enterprise Server installer.

The pre-installation configuration of the server is complete. Continue to Install or Upgrade/Migrate.

4

Install or Upgrade/Migrate

The chapter details a new installation of the Dell Enterprise Server or an upgrade/migration of an older Dell Enterprise Server to a newer Dell Enterprise Server.

To begin the installation/migration, select **one** option:

- New Installation
- Upgrade/Migration

New Installation

Before you begin, ensure that all Pre-Installation Configuration is complete.This is of particular importance if you intend to use the web browser version of the Silverlight Console or are deploying Dell Data Protection | Mobile Edition.

Read the *Release Notes* for any current workarounds or known issues related to Dell Enterprise Server installation.

Dell recommends that DB best practices are used for the Dell database and that Dell software is included in your organization's disaster recovery plan.

If you intend to deploy Dell components in the DMZ, ensure that they are properly protected against attacks.

For production, Dell strongly recommends installing the SQL Server on a dedicated server.

BEFORE YOU BEGIN:

As of v7.7, the Enterprise Server installation process contains a few changes from previous releases. You will notice a check box for "Front End" on the Set Up dialog. If your environment is installed on **one** server, simply ignore the check box and continue. If your environment is installed on **multiple** servers (Front End/DMZ/Internal *and* Back End/Enterprise), you will run this installer with the check box de-selected for your Back End/Enterprise server(s) and then run this installer again on your Front End/DMZ/Internal server(s) with the "Front End" check box selected. Selecting the check box installs only the "proxy" components (Security Server in Proxy Mode, Core Server in Proxy Mode, Device Server, and Policy Proxy).

First we will go through the install for the Main Server(s)/Back End and then we will go through the process for the Front End server(s).

Main Server(s)

1 In the Dell installation media, navigate to the Dell Enterprise Server directory. **Unzip** (NOT copy/paste or drag/drop) Dell Enterprise Server-x64 to the root directory of the server where you are installing Dell Data Protection | Enterprise Edition. ***Copying/pasting or dragging/dropping will produce errors and an unsuccessful installation.***

NOTE: Follow the same procedure for Dell Enterprise Server-x86 for the 32-bit installer.

2 Double-click **setup.exe**.

3 When the *InstallShield Wizard* displays, select the language for installation, then click **OK**.

4 If not already installed, a message may display, informing you that Microsoft Visual C++ 2010 Redistributable Package must be installed before continuing. Click **Install**.

5 When the *Welcome* dialog displays, click **Next**.

6 At the *License Agreement*, indicate acceptance, then click **Next**.

7 If you optionally completed step 14 in Pre-Installation Configuration, click **Next**. If not, enter the 32-character Product Key and then click **Next**. The Product Key is located in the file "*EnterpriseServerInstallKey.ini*".

8 Click **Next** to install the Dell Enterprise Server to the default location of C:\Program Files\Dell. Otherwise, click **Change** to select a different location, then click **Next**.

9 Select the Setup type (without the Front End check box being selected) and click **Next**.

If the **Complete** option is selected, all program features are installed. Continue to step 11.

The **Custom** option selection allows installation of only those program features desired. Continue to step 10.

10 At the *Custom Setup* dialog, choose the features you want to install. For a description of each feature and what it is required for, see Dell Component Descriptions.

Once the features are selected, click **Next**. Continue to step 11.

11 Verify that all fields are populated for each component. Leave the default port value as-is unless there is a conflict with an existing port.

If the "Works with Front End...." box is selected, on the next dialog, you will enter the fully qualified domain name for the Dell Security Server. If you have an external certificate that is being used with APNs, enter the fully qualified domain name specified in the certificate. If the box is not selected, then the field is not available on the next dialog. Click **Next**.

12 For the Front End Security Server host name, this relates to the previous dialog's "Works with Front End...." box. If the box was selected on the previous dialog, enter the fully qualified domain name for the Dell Security Server. If you have an external certificate that is being used with APNs, enter the fully qualified domain name specified in the certificate. If the box was not selected, then the field is not available. Verify that all other fields are populated for component. Leave the default port value as-is unless there is a conflict with an existing port. Click **Next**.

NOTE: The Message Broker Service does not allow the "_" (underscore) character in the fully qualified domain name.

13 In the Security Socket Layer and Host dialog, enter the fully qualified domain name of the back-end server and select the correct Server edition, **Enterprise Edition** or **Virtual Edition**.

14 You have a choice of SSL types to use. Select option "a" or "b" below:

a To use an existing certificate that was purchased from a CA authority, select the first option and click **Next**.

NOTE: To use this setting, the exported CA certificate being imported must have the full trust chain. If unsure, re-export the CA certificate and ensure that the following options are selected in the "Certificate Export Wizard":
– Personal Information Exchange - PKCS#12 (.PFX)
– Include all certificates in the certification path if possible
– Export all extended properties

Click **Browse** to enter the path to the certificate.

Enter the password associated with this certificate. The key store file must be .p12 or pfx. See How to Export a Certificate to .PFX Using the Certificate Management Console for instructions.

Click **Next**.

OR

b To create a self-signed certificate, select the second option and click Next.

At the *Set Up a Certificate Authority* dialog, enter the following information:

Fully qualified computer name (example: computername.domain.com)

Organizational Unit (example: Security)

Organization

City

State (full name)

Country: Two-letter country abbreviation

Click **Next**.

15 At the *Ready to Install the Program* dialog, click **Install** to begin installation.

16 When prompted, click **Finish** to complete the installation.

Do not reboot the server until Post-Installation Configuration tasks are complete. Rebooting now would cause the server to attempt to start Dell Services, which would be unsuccessful at this point.

Front End Server(s)

1 In the Dell installation media, navigate to the Dell Enterprise Server directory. **Unzip** (NOT copy/paste or drag/drop) Dell Enterprise Server-x64 to the root directory of the server where you are installing Dell Data Protection | Enterprise Edition. ***Copying/pasting or dragging/dropping will produce errors and an unsuccessful installation.***

NOTE: Follow the same procedure for Dell Enterprise Server-x86 for the 32-bit installer.

2 Double-click **setup.exe**.

3 When the *InstallShield Wizard* displays, select the language for installation, then click **OK**.

4 If not already installed, a message may display, informing you that Microsoft Visual C++ 2010 Redistributable Package must be installed before continuing. Click **Install**.

5 When the *Welcome* dialog displays, click **Next**.

6 At the *License Agreement*, indicate acceptance, then click **Next**.

7 If you optionally completed step 14 in Pre-Installation Configuration, click **Next**. If not, enter the 32-character Product Key and then click **Next**. The Product Key is located in the file "*EnterpriseServerInstallKey.ini*".

8 Click **Next** to install the Dell Enterprise Server to the default location of C:\Program Files\Dell. Otherwise, click **Change** to select a different location, then click **Next**.

9 Select **Complete** and select the Front End check box, to indicate that a Front End server will be used. Click **Next**. We recommend only selecting *Complete*. If you select *Custom*, you will need to de-select all of the components you do not want installed on the Front End. The Complete option automatically installs only the components that are appropriate for the Front End.

10 For the Security Server (in Proxy Mode), Core Server (in Proxy Mode), and Device Server (in Proxy Mode), verify that all fields are populated and correct for each component. Leave the default port value as-is unless there is a conflict with an existing port. For the *back end settings used by this server* area, enter the FQDNs of the Back End Servers so that the Front End Servers may communicate with them. All fields are required. Click **Next**.

NOTE: The Message Broker Service does not allow the "_" (underscore) character in the fully qualified domain name.

11 In the Security Socket Layer and Host dialog, enter the fully qualified domain name of the back-end server and select the correct Server edition, **Enterprise Edition** or **Virtual Edition**.

12 You have a choice of SSL types to use. Select option "a" or "b" below:

a To use an existing certificate that was purchased from a CA authority, select the first option and click **Next**.

NOTE: To use this setting, the exported CA certificate being imported must have the full trust chain. If unsure, re-export the CA certificate and ensure that the following options are selected in the "Certificate Export Wizard":
– Personal Information Exchange - PKCS#12 (.PFX)
– Include all certificates in the certification path if possible
– Export all extended properties

Click **Browse** to enter the path to the certificate.

Enter the password associated with this certificate. The key store file must be .p12 or pfx. See How to Export a Certificate to .PFX Using the Certificate Management Console for instructions.

Click **Next**.

OR

b To create a self-signed certificate, select the **second** option and click **Next**.

At the *Set Up a Certificate Authority* dialog, enter the following information:

Fully qualified computer name (example: computername.domain.com)

Organizational Unit (example: Security)

Organization

City

State (full name)

Country: Two-letter country abbreviation

Click **Next**.

13 At the *Ready to Install the Program* dialog, click **Install** to begin installation.

14 When prompted, click **Finish** to complete the installation.

15 Go to <Security Server install dir>\conf\ and open the application.properties file.

Locate publicdns.server.host and set the name to an externally resolvable host name.

Locate publicdns.server.port and set the port (the default is 8443).

Do not reboot the server until Post-Installation Configuration tasks are complete. Rebooting now would cause the server to attempt to start Dell Services, which would be unsuccessful at this point.

—

The rest of this chapter details the process for an upgrade/migration and may be ignored. Continue to Post-Installation Configuration.

Upgrade/Migration

Before you begin, ensure that all Pre-Installation Configuration is complete.This is of particular importance if you intend to use the web browser version of the Silverlight Console or are deploying Dell Data Protection | Mobile Edition.

Read the *Release Notes* for any current workarounds or known issues related to Dell Enterprise Server installation.

Dell recommends that DB best practices are used for the Dell database and that Dell software is included in your organization's disaster recovery plan.

If you intend to deploy Dell components in the DMZ, ensure that they are properly protected against attacks.

For production, Dell recommends installing the SQL Server on a dedicated server.

To leverage full capabilities of policies, we recommend updating to the most current versions of both the Dell Enterprise Server and Clients.

Dell Enterprise Server v8.x supports:

- Dell Data Protection | Enterprise Edition (Windows clients) v7.x/8.x
- Dell Data Protection | Enterprise Edition (SED clients) v8.x
- Dell Data Protection | Authentication v8.x
- Dell Data Protection | BitLocker Manager v7.2~7.x/8.x
- Dell Data Protection | Cloud Edition v8.x
- Dell Data Protection | Enterprise Edition (Mac clients) v7.x/8.x
- Dell Data Protection | Mobile Edition v7.x/8.x
- Upgrade/Migration from Dell Enterprise Server v7.x

When upgrading/migrating your Dell Enterprise Server to a version that includes new policies that are introduced in that version, commit updated policy after upgrade/migration, to ensure that your preferred policy settings are implemented for the new policies, rather than default values.

In general, our recommended upgrade path is to upgrade/migrate the Dell Enterprise Server and its components, followed by Client installation/upgrade.

BEFORE YOU BEGIN:

As of v7.7, the Enterprise Server upgrade/migration process contains a few changes from previous releases. You will notice a check box for "Front End" on the Set Up dialog. If your environment is installed on **one** server, simply ignore the check box and continue. If your environment is installed on **multiple** servers (Front End/DMZ/Internal *and* Back End/Enterprise), you will run this installer with the check box de-selected for your Back End/Enterprise server(s) and then run this installer again on your Front End/DMZ/Internal server(s) with the "Front End" check box selected. Selecting the check box installs only the "proxy" components (Security Server in Proxy Mode, Core Server in Proxy Mode, Device Server, and Policy Proxy).

After publishing policies, backing up the database, and uninstalling the existing Server, we will go through the install for the Main Server(s)/Back End and then we will go through the process for the Front End server(s).

Main Server(s)

To begin the upgrade/migration:

1. If you have any pending policies: As a Dell Administrator, log in to the Dell Remote Management Console.
2. In the left menu, click **Actions > Commit Policies**.
3. Click **Apply Changes**.
4. When the commit is complete, log off the Dell Remote Management Console.
5. From the Windows *Start* menu, click **Start > Run**. Type *services.msc* and click **OK**. When *Services* opens, navigate to each Dell Service and click **Stop the service**.
6. Back up your entire existing installation (including the SQL database) to an alternate location. Several files from your existing installation will be needed after the upgrade/migration process is complete.
7. Uninstall your existing Dell Enterprise Server installation:
   - Navigate to *Add/Remove Programs* in the Control Panel.
   - Locate Dell Enterprise Server, click **Change/Remove** and follow the prompts.
   - Once the uninstall is complete, reboot the server.
   - Ensure the directories below no longer exist (if so manually delete).

     *\Program Files\Dell

     *\ProgramData\Dell
8. In the Dell installation media, navigate to the Dell Enterprise Server directory. **Unzip** (NOT copy/paste or drag/drop) Dell Enterprise Server-x64 to the root directory of the server where you are installing Dell Data Protection | Enterprise Edition. ***Copying/pasting or dragging/dropping will produce errors and an unsuccessful installation.***

NOTE: Follow the same procedure for Dell Enterprise Server-x86 for the 32-bit installer.

9. Double-click **setup.exe**.
10. When the *InstallShield Wizard* displays, select the language for installation, then click **OK**.
11. If not already installed, a message may display, informing you that Microsoft Visual C++ 2010 Redistributable Package must be installed before continuing. Click **Install**.
12. When the *Welcome* dialog displays, click **Next**.
13. At the *License Agreement*, indicate acceptance, then click **Next**.
14. If you optionally completed step 14 in Pre-Installation Configuration, click **Next**. If not, enter the 32-character Product Key and then click **Next**. The Product Key is located in the file "EnterpriseServerInstallKey.ini".
15. Click **Next** to install the Dell Enterprise Server to the default location of C:\Program Files\Dell. Otherwise, click **Change** to select a different location, then click **Next**.
16. Select the Setup type (without the Front End check box being selected) and click **Next**.

    If the **Complete** option is selected, all program features are installed. Continue to step 18.

    The **Custom** option selection allows installation of only those program features desired. Continue to step 17.
17. At the *Custom Setup* dialog, choose the features you want to install. For a description of each feature and what it is required for, see Dell Component Descriptions.

    Once the features are selected, click **Next**. Continue to step 18.
18. Verify that all fields are populated for each component. Leave the default port value as-is unless there is a conflict with an existing port. If the "Works with Front End..." box is selected, on the next dialog, you will enter the fully qualified domain name for the Dell Security Server. If you have an external certificate that is being used with APNs, enter the fully qualified domain name specified in the certificate. If the box is not selected, then the field is not available on the next dialog. Click **Next**.

19 For the Front End Security Server host name, this relates to the previous dialog's "Works with Front End..." box. If the box was selected on the previous dialog, enter the fully qualified domain name for the Dell Security Server. If you have an external certificate that is being used with APNs, enter the fully qualified domain name specified in the certificate. If the box was not selected, then the field is not available. Verify that all other fields are populated for component. Leave the default port value as-is unless there is a conflict with an existing port. Click **Next**.

NOTE: The Message Broker Service does not allow the "_" (underscore) character in the fully qualified domain name.

20 In the Security Socket Layer and Host dialog, enter the fully qualified domain name of the back-end server and select the correct Server edition, **Enterprise Edition** or **Virtual Edition**.

21 You have a choice of SSL types to use. Select option "a" or "b" below:

a To use an existing certificate that was purchased from a CA authority, select the first option and click **Next**.

NOTE: To use this setting, the exported CA certificate being imported must have the full trust chain. If unsure, re-export the CA certificate and ensure that the following options are selected in the "Certificate Export Wizard":
– Personal Information Exchange - PKCS#12 (.PFX)
– Include all certificates in the certification path if possible
– Export all extended properties

Click **Browse** to enter the path to the certificate.

Enter the password associated with this certificate. The key store file must be .p12 or pfx. See How to Export a Certificate to .PFX Using the Certificate Management Console for instructions.

Click **Next**.

OR

b To create a self-signed certificate, select the **second** option and click **Next**.

At the *Set Up a Certificate Authority* dialog, enter the following information:

Fully qualified computer name (example: computername.domain.com)

Organizational Unit (example: Security)

Organization

City

State (full name)

Country: Two-letter country abbreviation

Click **Next**.

22 At the *Ready to Install the Program* dialog, click **Install** to begin installation.

23 When prompted, click **Finish** to complete the installation.

Do not reboot the server until Post-Installation Configuration tasks are complete. Rebooting now would cause the server to attempt to start Dell Services, which would be unsuccessful at this point.

24 In your backed up installation, copy/paste: <Compatibility Server install dir>\conf\secretKeyStore to the new installation:

<Compatibility Server install dir>\conf\secretKeyStore

25 In the new installation, open <Compatibility Server install dir>\conf\server_config.xml and replace the **server.pass** value with the value from the backed up <Compatibility Server install dir>\conf\server_config.xml, as follows:

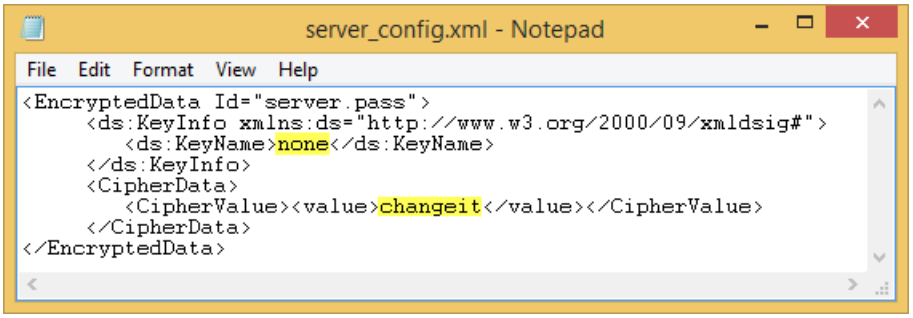
Instructions for server.pass:

If you know the password, refer to the example server_config.xml file in Figure 4-1, and make the following changes:

- Edit the *KeyName* from **CFG_KEY** value to **none**
- Enter the plain text password and enclose it between *<value>* *</value>*, which in this example is **<value>changeit</value>**

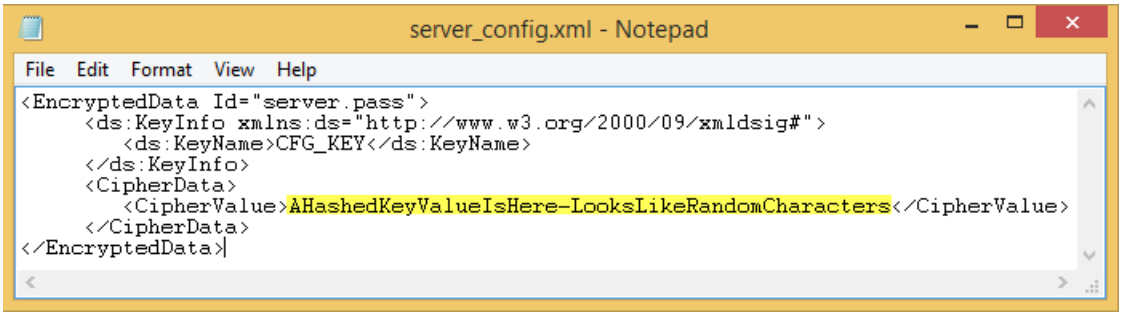
When the Dell Enterprise Server starts, the plain text password is hashed, and the hashed value replaces the plain text.

Figure 4-1. Known Password



If you do not know the password, cut and paste the section similar to the section shown in Figure 4-2 from the backed up <Compatibility Server install dir>\conf\server_config.xml file into the corresponding section in the new *server_config.xml* file.

Figure 4-2. Unknown Password



Save and close the file.

NOTE: Do not attempt to change the Dell Enterprise Server password by editing the server.pass value in server_config.xml at any other time. If you change this value, you lose access to the database.

Front End Server(s)

1 In the Dell installation media, navigate to the Dell Enterprise Server directory. **Unzip** (NOT copy/paste or drag/drop) Dell Enterprise Server-x64 to the root directory of the server where you are installing Dell Data Protection | Enterprise Edition. ***Copying/pasting or dragging/dropping will produce errors and an unsuccessful installation.***

NOTE: Follow the same procedure for Dell Enterprise Server-x86 for the 32-bit installer.

2 Double-click **setup.exe**.

3 When the *InstallShield Wizard* displays, select the language for installation, then click **OK**.

4 If not already installed, a message may display, informing you that Microsoft Visual C++ 2010 Redistributable Package must be installed before continuing. Click **Install**.

5 When the *Welcome* dialog displays, click **Next**.

6 At the *License Agreement*, indicate acceptance, then click **Next**.

7 If you optionally completed step 14 in Pre-Installation Configuration, click **Next**. If not, enter the 32-character Product Key and then click **Next**. The Product Key is located in the file "EnterpriseServerInstallKey.ini".

8 Click **Next** to install the Dell Enterprise Server to the default location of C:\Program Files\Dell. Otherwise, click **Change** to select a different location, then click **Next**.

9 Select **Complete** and select the Front End check box. Click **Next**. We recommend only selecting *Complete*. If you select *Custom*, you will need to de-select all of the components you do not want installed on the Front End. The Complete option automatically installs only the components that are appropriate for the Front End.

10 For the Security Server (in Proxy Mode), Core Server (in Proxy Mode), and Device Server (in Proxy Mode), verify that all fields are populated and correct for each component. Leave the default port value as-is unless there is a conflict with an existing port. For the *back end settings used by this server* area, enter the FQDNs of the Back End Servers so that the Front End Servers may communicate with them. All fields are required. Click **Next**.

NOTE: The Message Broker Service does not allow the "_" (underscore) character in the fully qualified domain name.

11 In the Security Socket Layer and Host dialog, enter the fully qualified domain name of the back-end server and select the correct Server edition, **Enterprise Edition** or **Virtual Edition**.

12 You have a choice of SSL types to use. Select option "a" or "b" below:

a To use an existing certificate that was purchased from a CA authority, select the first option and click **Next**.

NOTE: To use this setting, the exported CA certificate being imported must have the full trust chain. If unsure, re-export the CA certificate and ensure that the following options are selected in the "Certificate Export Wizard":
– Personal Information Exchange - PKCS#12 (.PFX)
– Include all certificates in the certification path if possible
– Export all extended properties

Click **Browse** to enter the path to the certificate.

Enter the password associated with this certificate. The key store file must be .p12 or pfx. See How to Export a Certificate to .PFX Using the Certificate Management Console for instructions.

Click **Next**.

OR

b To create a self-signed certificate, select the **second** option and click **Next**.

At the *Set Up a Certificate Authority* dialog, enter the following information:

Fully qualified computer name (example: computername.domain.com)

Organizational Unit (example: Security)

Organization

City

State (full name)

Country: Two-letter country abbreviation

Click **Next**.

13 At the *Ready to Install the Program* dialog, click **Install** to begin installation.

14 When prompted, click **Finish** to complete the installation.

15 Go to <Security Server install dir>\conf\ and open the application.properties file.

Locate publicdns.server.host and set the name to an externally resolvable host name.

Locate publicdns.server.port and set the port (the default is 8443).

Do not reboot the server until Post-Installation Configuration tasks are complete. Rebooting now would cause the server to attempt to start Dell Services, which would be unsuccessful at this point.

Upgrade/migration tasks are now complete. Continue to Post-Installation Configuration.

5

Post-Installation Configuration

Read the *Release Notes* for current workarounds or known issues related to Dell Enterprise Server configuration.

Whether you are installing the Dell Enterprise Server for the first time or are upgrading an existing installation, some components of your environment must be configured.

EAS Management Installation and Configuration

This section needs to be completed if you intend to use Dell Data Protection | Mobile Edition. If not, omit this section and continue to Dell Security Server in DMZ Mode Configuration.

Prerequisites

- The logon account for the EAS Mailbox Manager Service must be an account with permissions to create/modify Exchange ActiveSync policy, assign policies to user mailboxes, and query information about ActiveSync devices.
- The EAS Configuration Utility must be run with Admin permissions to modify files and restart Services.
- Network connection to the Dell Policy Proxy is required.
- Have the FQDN of the Dell Policy Proxy available.
- Have the Dell Policy Proxy port number available.
- Microsoft Message Queuing (MSMQ) must already be installed/configured on the server hosting the Exchange environment. If not, see Install/Configure Microsoft Message Queuing (MSMQ).

During the Deployment Process

If you intend to use Exchange ActiveSync to manage mobile devices through Dell Data Protection | Mobile Edition, your Exchange Server environment must be configured.

Install EAS Device Manager

1. In the Dell installation media, navigate to the EAS Management folder. In the EAS Device Manager folder, copy setup.exe to your *Exchange Client Access Server(s)*.
2. Double-click **setup.exe** to begin the installation. If your environment includes more than one *Exchange Client Access Server*, run this installer on each one.
3. Select the language for installation, then click **OK**.
4. Click **Next** when the *Welcome* screen displays.
5. Read the license agreement, agree to the terms, and click **Next**.
6. Click **Next** to install EAS Device Manager in the default location of C:\Inetpub\wwwroot\Dell\EAS Device Manager\.
7. Click **Install** at the *Ready to Begin Installation* screen.

   A status window displays the installation progress.
8. If desired, check the box to show the Windows Installer log and click **Finish**.

Install EAS Mailbox Manager

1. In the Dell installation media, navigate to the EAS Management folder. In the EAS Mailbox Manager folder, copy setup.exe to your *Exchange Mailbox Server(s)*.
2. Double-click **setup.exe** to begin the installation. If your environment includes more than one *Exchange Mailbox Server*, run this installer on each one.

3 Select the language for installation, then click **OK**.

4 Click **Next** when the *Welcome* screen displays.

5 Read the license agreement, agree to the terms, and click **Next**.

6 Click **Next** to install EAS Mailbox Manager in the default location of C:\Program Files\Dell\EAS Mailbox Manager\.

7 At the Logon Information screen, enter the credentials of the user account that will logon to use this Service.

User Name: DOMAIN\Username

Password: password associated with this user name

Click **Next**.

8 Click **Install** at the *Ready to Begin Installation* screen.

A status window displays the installation progress.

9 If desired, check the box to show the Windows Installer log and click **Finish**.

Use the EAS Configuration Utility

10 On the same computer, go to **Start > Dell > EAS Configuration Utility > EAS Configuration** to run the EAS Configuration Utility.

11 Click **Setup** to configure EAS Management Settings.

12 Enter the following information:

FQDN of the Dell Policy Proxy

Dell Policy Proxy Port (the default port is 8090)

Dell Policy Proxy Polling Interval (the default is 1 minute)

Select the box to run EAS Device Manager in report-only mode (recommended during deployment)

NOTE: The Report-only mode allows unknown devices/users to have access to Exchange ActiveSync, but still reports the traffic to you. Once your deployment is up and running, you can change this setting to tighten security.

Click **OK**.

13 A success message displays. Click **Yes** to re-start IIS and EAS Mailbox Manager Services.

14 Click **Quit** when finished.

After the Deployment Process

Once your deployment is up and running, and you are ready to tighten security, follow the steps below.

On your Exchange Mailbox Server(s)

1 Go to **Start > Dell > EAS Configuration Utility > EAS Configuration** to run the EAS Configuration Utility.

2 Click **Setup** to configure EAS Management Settings.

3 Enter the following information:

FQDN of the Dell Policy Proxy

Dell Policy Proxy Port (the default port is 8090)

Dell Policy Proxy Polling Interval (the default is 1 minute)

De-select the box to run EAS Device Manager in report-only mode

Click **OK**.

4 A success message displays. Click **Yes** to re-start IIS and EAS Mailbox Manager Services.

5 Click **Quit** when finished.

Continue to Dell Security Server in DMZ Mode Configuration.

Dell Security Server in DMZ Mode Configuration

If the Dell Security Server is deployed in a DMZ and a private network, and only the DMZ server has a domain certificate from a trusted Certificate Authority (CA), some manual steps are needed to add the trusted certificate into the Java keystore of the private network Dell Security Server.

If a trusted certificate is being used, omit this section and continue to APNs Enrollment.

NOTE: We highly recommend the use of domain certificates from a trusted Certificate Authority for both DMZ and private network servers.

Use Keytool to Import the DMZ Domain Certificate

IMPORTANT: Backup the existing Dell Security Server cacerts before continuing with the Keytool instructions.If a configuration error is made, you can revert back to the saved file.

Assumptions

- Dell Security Server was installed with an untrusted certificate.
- Dell Security Server in DMZ Mode was installed using a signed certificate (Entrust, Verisign, etc.)
- A .pfx certificate file is available. If your certificate needs to be converted to .pfx, see How to Export a Certificate to .PFX Using the Certificate Management Console.

Process

1 Add Keytool to the system path.

```
set path=%path%;<Dell Java Install Dir>\bin
```

2 Use Keytool to list the contents of the trusted domain certificate that you want to import. Take note of the Alias Name listed.

```
keytool -list -v -keystore "C:\<path-to-pfx>\SignedCert.pfx -storetype PKCS12
```

3 Use Keytool to import the contents of the signed certificate into the Dell Security Server's cacerts file:

```
keytool -importkeystore -v -srckeystore "C:\<path-to-source-file>\SignedCert.pfx"
-srcstoretype PKCS12 -srcalias AliasName -destkeystore "C:\<path-to-dest-cacert>\cacerts"
-deststorepass changeit -destalias AliasName -destkeypass changeit
```

For -srcalias, you will need to gather this information from the exported contents of the signed certificate.

For -destalias, this can be any location you choose.

4 Backup and replace the current cacerts file in the <Security Server install dir>\conf\ directory with this newly created cacerts file on the Dell Security Server.

Modify application.properties File

Modify the application.properties file to specify the alias of the signing cert.

1 Go to <Security Server install dir>\conf\application.properties

2 Modify the follow information:

keystore.alias.signing=<Change this value to the value of step 3 above for `-destalias>`

3 Restart the Dell Security Server Service.

Continue to APNs Enrollment.

APNs Enrollment

If you intend to use Dell Data Protection | Mobile Edition with iOS devices, the APNs Enrollment wizard must be used to:

- Create a CSR
- Create an Apple Push Certificate
- Upload a Push Certificate

If you do not intend to use Dell Data Protection | Mobile Edition with iOS devices, omit this section and continue to Use Windows Authentication.

The Apple Push Notification service (APNs) enables secure communication to iOS devices over-the-air. APNs is used to send notification for an iOS device to check in with the Dell Enterprise Server. The APNs only sends notification to the device, no data is sent.

Process

1 Open a browser and go to https://<FQDN-of-security-server>:8443/csrweb.

2 On the APNs Enrollment Wizard Login dialog, enter your Dell Administrator credentials and click **Login**.

3 A dialog displays that describes the steps you are about to take. Click **Next**.

Step I: Create CSR

4 Enter the following information:

Email: The email address can be any UPN, but we recommend using an account for the administrator that will be maintaining the APNs certificate.

Common Name: Enter the Common Name associated with this email address.

Click **Generate CSR**.

5 After you generate a CSR, save the file to an easily accessible location.

6 Click **Next**.

Step II: Create Apple Push Certificate

7 Click the link for the **Apple Push Certificate Portal**. Login with your Apple ID and password.

8 Read the Terms of Use, indicate acceptance, and click **Accept**.

9 Click **Browse** and then **Upload** the CSR you just created.

10 On the *Certificates for Third-Party Servers* page, click **Download**. Save the file to an easily accessible location.

11 Return to the APNs Enrollment Wizard and click **Next**.

Step III: Upload Push Certificate

12 Enter the following information (use the same credentials that were used in Step I: Create CSR).

Email:

Common Name:

Push Cert File: Click **Browse** to locate the file saved in step 10. Click **Upload**.

13 A success message displays. Click **Finish**.

Enrollment of the APNs Certificate with the Dell Server is complete.

Continue to Use Windows Authentication.

Use Windows Authentication

If you want to use Windows Authentication instead of SQL Authentication, complete the following steps before running the Dell Server Configuration Tool. If you do not intend to use Windows Authentication, continue to Use the Dell Server Configuration Tool.

1 Create a Windows domain account with privileges to serve as Dell database owner and this account will also need to be a member of the Enterprise Server's Local Administrators Group. This account is used to run Dell Services, so it is important that potential password issues are prevented. Ensure that the following password settings are applied:

   a Ensure the following option is *NOT* selected:
   User Must Change Password on next Login

   b Ensure the following options *ARE* selected:
   User cannot change password (this setting is optional, but ensures that a user does not accidentally change this password)

   and

   Password never expires

Configure the Dell Compatibility Server Service to run using the Windows domain account you set up:

2 Go to **Start** > **Run**. Type *services.msc* and click **OK**.

3 When *Services* opens, highlight Dell Compatibility Server. Right-click the entry and select **Properties**.

4 On the *Log On* tab, select **This account**. Browse to locate the Windows domain account you set up. The format should be DomainName\AdministratorName or administrator@domainname.com.

5 Type the password for this Windows domain account and confirm it.

6 Click **OK**.

Configure the Dell Compliance Reporter Service to run using the Windows domain account you set up:

1 Go to **Start** > **Run**. Type *services.msc* and click **OK**.

2 When *Services* opens, highlight Dell Compliance Reporter. Right-click the entry and select **Properties**.

3 On the *Log On* tab, select **This account**. Browse to locate the Windows domain account you set up. The format should be DomainName\AdministratorName or administrator@domainname.com.

4 Type the password for this Windows domain account and confirm it.

5 Click **OK**.

Configure the Dell Core Server Service to run using the Windows domain account you set up:

1 Go to **Start** > **Run**. Type *services.msc* and click **OK**.

2 When *Services* opens, highlight Dell Core Server. Right-click the entry and select **Properties**.

3 On the *Log On* tab, select **This account**. Browse to locate the Windows domain account you set up. The format should be DomainName\AdministratorName or administrator@domainname.com.

4 Type the password for this Windows domain account and confirm it.

5 Click **OK**.

Configure the Dell Identity Server to run using the Windows domain account you set up:

1 Go to **Start** > **Run**. Type *services.msc* and click **OK**.

2 When *Services* opens, highlight Dell Core Server. Right-click the entry and select **Properties**.

3 On the *Log On* tab, select **This account**. Browse to locate the Windows domain account you set up. The format should be DomainName\AdministratorName or administrator@domainname.com.

4 Type the password for this Windows domain account and confirm it.

5 Click **OK**.

Configure the Dell Key Server to run using the Windows domain account you set up:

1 Go to **Start** > **Run**. Type *services.msc* and click **OK**.
2 When *Services* opens, highlight Dell Key Server. Right-click the entry and select **Properties**.
3 On the *Log On* tab, select **This account**. Browse to locate the Windows domain account you set up. The format should be DomainName\AdministratorName or administrator@domainname.com.
4 Type the password for this Windows domain account and confirm it.
5 Click **OK**.

Configure the Dell Message Broker Service to run using the Windows domain account you set up:

1 Go to **Start** > **Run**. Type *services.msc* and click **OK**.
2 When *Services* opens, highlight Dell Message Broker. Right-click the entry and select **Properties**.
3 On the *Log On* tab, select **This account**. Browse to locate the Windows domain account you set up. The format should be DomainName\AdministratorName or administrator@domainname.com.
4 Type the password for this Windows domain account and confirm it.
5 Click **OK**.

Configure the Dell Security Server Service to run using the Windows domain account you set up:

1 Go to **Start** > **Run**. Type *services.msc* and click **OK**.
2 When *Services* opens, highlight Dell Security Server. Right-click the entry and select **Properties**.
3 On the *Log On* tab, select **This account**. Browse to locate the Windows domain account you set up. The format should be DomainName\AdministratorName or administrator@domainname.com.
4 Type the password for this Windows domain account and confirm it.
5 Click **OK**.

Configure Dell Compliance Reporter to use Windows Authentication:

- As of v8.1, Compliance Reporter is configured to use Windows Authentication out-of-the-box. No configuration is needed.

Continue to Use the Dell Server Configuration Tool.

Use the Dell Server Configuration Tool

Whether a new install or an upgrade/migration from a previous version, the Dell Server Configuration Tool must be used to configure your environment.

The Dell Core Server and Dell Compatibility Server cannot run simultaneously with the Dell Server Configuration Tool. Stop the Dell Core Server Service and Dell Compatibility Server Service in *Services* (Start > Run. Type *services.msc*) prior to starting the Dell Server Configuration Tool.

The Dell Server Configuration Tool allows you to:

- Configure and *initialize* your Microsoft SQL database to allow communication with Dell Servers during a new installation of the Dell Enterprise Server.

  OR

  Configure and *migrate* your Microsoft SQL database to allow communication with Dell Servers during an upgrade/migration of Dell Enterprise Server.
- Configure certificates.
- Configure settings for the web browser version of the Silverlight Console and Dell Manager Trust Validation.
- Configure SMTP settings for Dell Data Protection I Cloud Edition
- Import a Dell Manager certificate.

To begin, select either:

- Configure a New Installation
- Configure a Migration

Configure a New Installation

1 Launch the Dell Server Configuration Tool. Go to **Start > Programs > Dell > Enterprise Edition > Server Configuration Tool > Run Server Configuration Tool**.

2 You may get informational messages stating that your database configuration settings do not match. These messages are for information only and are not a cause for concern. If prompted, click **OK** for each message.

3 Click the *Information* tab.

This tab is for information only and cannot be edited. All fields are pre-populated.

Core Server:	displays the installed location of the Dell Core Server.
Legacy Server:	displays the installed location of the Dell Compatibility Server.
Security Server:	displays the installed location of the Dell Security Server.
Messaging Service	displays the installed location of the Dell Messaging Service.
Compliance Reporter	displays the installed location of the Compliance Reporter.
Identity Server	displays the installed location of the Identity Server.
Schema Version:	displays the current database schema version.
Supported Versions:	displays the previous versions supported to migrate to the current version.

4 Click the *Database* tab.

a In the *Server Name:* field, enter the fully qualified domain name (if there is an instance name, include it) of the server hosting the database. For example, SQLTest.domain.com\DellDB.

Dell recommends using a fully qualified domain name, although an IP address may be used.

b In the *Database:* field, enter the name of the database.

c In the *Authentication:* field, select either **Windows Authentication** or **SQL Server Authentication**. If you choose Windows Authentication, the same credentials that were used to log in to Windows will be used for authentication (User Name and Password fields will not be editable).

d In the *User Name:* field, enter the appropriate username associated with this database.

e In the *Password:* field, enter the password for the username listed in the UserName field.

f From the top menu, select **Configuration > Save**. If prompted, confirm the save.

5 Test Database Configuration.

a From the top menu, select **Actions > Test Database Configuration**. The Configuration Wizard launches.

NOTE: The database cannot be initialized until after the database configuration tests have passed.

b At the *Configuration Test* window, read the test information and click **Next**.

c If you chose Windows Authentication in the *Database* tab, you can optionally enter alternate credentials to allow the use of the same credentials that will be used to run the Dell Enterprise Server. Click **Next**.

d At the *Test Configuration* window, the results of the Test Connection Settings, Compatibility Test, and the Database Initialized Test display.

You may get a failed test result for the Database Initialized Test, which is correct – this database has not been initialized yet. You cannot initialize this database until the two other tests, Test Connection Settings and Compatibility Test, have a result of Passed.

Click **Finish**.

e From the top menu, select **Configuration > Save**. If prompted, confirm the save.

6 Initialize Database.

a From the top menu, select **Actions > Initialize Database**. The Configuration Wizard launches.

NOTE: If you are reinstalling or upgrading the Dell Enterprise Server, initializing the database erases all data, including key material, user states, and administrators. Initialize the database in a new installation only. If you are reinstalling or upgrading, use the instructions in Configure a Migration.

b At the *Initialize Enterprise Database* window, a warning displays. Confirm that you have either backed up the entire database or confirm that a backup does not need to be made of your existing database. Click **Next**.

c At the *Initialize Enterprise Database* window, read the information and click **Next**.

At the *Initializing Database* window, informational messages display the status of the initialization.

When complete, check for errors.

NOTE: An error message identified by , signifies that a database task has failed and corrective action needs to be taken before the database can be properly initialized. Click Finish, correct the database errors, and reinitiate the instructions in this section.

d Click **Finish**.

e From the top menu, select **Configuration** > **Save**. If prompted, confirm the save.

7 Configure Certificates.

The first time you run the Dell Server Configuration Tool for initial Dell Enterprise Server setup, certificates must be configured for the Dell Compatibility Server, Dell Core Server, and Message Security.

You have a choice of which type of certificates to use – self-signed or signed:

– **Self-signed** certificates are signed by their own creator. Self-signed certificates are appropriate for pilots, POCs, etc. For a production environment, Dell recommends public CA-signed or domain-signed certificates.

– **Signed** (public CA-signed or domain-signed) certificates are signed by a public CA or a domain. In the case of certificates that are signed by a public certificate authority (CA), the certificate of the signing CA will, usually, already exist in the Microsoft certificate store and therefore, the chain of trust will be automatically established. For domain CA-signed certificates, if the workstation has been joined to the domain, the signing CA certificate from the domain will have been added to the workstation's Microsoft certificate store, thereby also creating a chain of trust.

The components that are affected by certificate configuration:

– Java Services (for instance, Dell Device Server, Dell Console Web Services, and so on)

– .NET Applications (Dell Core Server)

– Validation of smart cards used for Preboot Authentication (Dell Security Server)

– Importing of private encryption keys to be used for signing policy bundles being sent to Dell Manager. Dell Manager performs SSL validation for remotely-managed Enterprise Edition clients with Hardware Crypto Accelerators, self-encrypting drives, or BitLocker Manager.

– Client Workstations:

  · Workstations running the web browser version of the Silverlight Console

  · Workstations running Dell Data Protection | BitLocker Manager

  · Workstations running Dell Data Protection | Enterprise Edition (Windows clients)

Information regarding which type of certificates to use:

Preboot Authentication using smart cards requires SSL validation with the Dell Security Server. Dell Manager performs SSL validation when connecting to the Dell Core Server. For these types of connections, the signing CA will need to be in the keystore (either the Java keystore or the Microsoft keystore, depending on which Dell Server component is being discussed). If self-signed certificates are chosen, the following options are available:

– Validation of smart cards used for Preboot Authentication:

  · Import the "Root Agency" signing certificate and full chain of trust into the Dell Security Server Java keystore. For more information, see Create a Self-Signed Certificate and Generate a Certificate Signing Request. The full chain of trust must be imported.

– Dell Manager:

  · Insert the "Root Agency" signing certificate (from the self-signed certificate generated) into the workstation's "Trusted Root Certification Authorities" (for "local computer") in the Microsoft keystore.

  · Modify the behavior of Dell Manager to not perform SSL validation. To turn off Dell Manager SSL trust validation, check **Disable Trust Chain Check** on the *Settings* tab.

  The client computer also must have the following registry entry to disable trust validation:

HKLM\System\CurrentControlSet\Services\CredMgmtAgent\Parameters\DisableSSLCertTrust (DWORD (32-bit) Value)=1

Disabling trust validation lessens security, but allows you to use a self-signed certificate for pilots, POCs, etc. For a production environment, Dell recommends public CA-signed or domain-signed certificates.

– Workstations running the web browser version of the Silverlight Console:

·Insert the "Root Agency" signing certificate (from Intermediate Certification Authorities) into the workstation's "Trusted Root Certification Authorities" (for "local computer") in the Microsoft keystore.

There are two methods to create a certificate – *Express* and *Advanced*.

Choose **one** method:

· Express – Choose this method to generate a self-signed certificate for all components. This is the easiest method.

· Advanced – Choose this method to configure each component separately.

Express

a From the top menu, select **Actions > Configure Certificates**.

b When the Configuration Wizard launches, select **Express** and click **Next**. The information from the self-signed certificate that was created when installing the Enterprise Server will be used, if available.

c From the top menu, select **Configuration > Save**. If prompted, confirm the save.

Certficate set up is complete. The rest of this section details the Advanced method of creating a certificate and may be ignored.

If your deployment includes Dell Manager, continue to step 8 on page 50.

If your deployment does **not** include Dell Manager, continue to step 9 on page 51.

Advanced

There are two paths to create a certificate – *Generate Self-Signed Certificate* and *Use Current Settings*. Choose **one** path:

· Path 1 – Generate Self-Signed Certificate

· Path 2 – Use Current Settings

Path 1 – Generate Self-Signed Certificate

a From the top menu, select **Actions > Configure Certificates**.

b When the Configuration Wizard launches, select **Advanced** and click **Next**.

c Select **Generate Self-Signed Certificate** and click **Next**. The information from the self-signed certificate that was created when installing the Enterprise Server will be used, if available.

d From the top menu, select **Configuration > Save**. If prompted, confirm the save.

Certficate set up is complete. The rest of this section details the other method of creating a certificate and may be ignored.

If your deployment includes Dell Manager, continue to step 8 on page 50.

If your deployment does **not** include Dell Manager, continue to step 9 on page 51.

Path 2 – Use Current Settings

a From the top menu, select **Actions > Configure Certificates**.

b When the Configuration Wizard launches, select **Advanced** and click **Next**.

c Select **Use Current Settings** and click **Next**.

d At the *Compatibility Server SSL Certificate* window, select **Generate Self-Signed Certificate** and click **Next**. The information from the self-signed certificate that was created when installing the Enterprise Server will be used, if available.

Click **Next**.

e At the *Core Server SSL Certificate* window, select one of the following:

– *Select Certificate* – Select this option to use an existing certificate. Click **Next**.

Browse to the location of the existing certificate, enter the password associated with the existing certificate, and click **Next**.

Click **Finish** when complete.

– *Generate Self-Signed Certificate* – The information from the self-signed certificate that was created when installing the Enterprise Server will be used, if available. If you select this option, the Message Security Certificate window does not display (the window does display if you select option *Use Current Settings*) and the certificate created for the Dell Compatibility Server is used.

Verify that the fully qualified computer name is correct. Click **Next**.

A warning message displays, telling you that a certificate by the same name already exists. When asked if you would like to use it, click **Yes**.

Click **Finish** when complete.

– *Use Current Settings* – Select this option to change a setting on a certificate anytime after the initial configuration of the Dell Enterprise Server. Selecting this option leaves your already configured certificate in place. Selecting this option advances you to the Message Security Certificate window.

At the Message Security Certificate, select **one** of the following:

·*Select Certificate* – Select this option to use an existing certificate. Click **Next**.

Browse to the location of the existing certificate, enter the password associated with the existing certificate, and click **Next**.

Click **Finish** when complete.

·*Generate Self-Signed Certificate* – The information from the self-signed certificate that was created when installing the Enterprise Server will be used, if available.

Click **Next**.

Click **Finish** when complete.

f From the top menu, select **Configuration > Save**. If prompted, confirm the save.

Certficate set up is complete.

If your deployment includes Dell Manager, continue to step 8.

If your deployment does **not** include Dell Manager, continue to step 9.

8 Import Dell Manager Certificate.

If your deployment includes Enterprise Edition remotely-managed clients with Hardware Crypto Accelerators, self-encrypting drives, or BitLocker Manager, you must import your newly created (or existing) certificate. The Dell Manager certificate is used as a vehicle to protect the private key which is used to sign the policy bundles being sent to Enterprise Edition remotely-managed clients and BitLocker Manager. This certificate can be independent of any of the other certificates. Additionally, if this key is compromised it can be replaced with a new key, and Dell Manager will request a new public key if it cannot decrypt the policy bundles.

a Open the Microsoft Management Console.

b Click **File > Add/Remove Snap-in**.

c Click **Add**.

d At the *Add Standalone Snap-in* window, select **Certificates** and click **Add**.

e Select **Computer Account** and click **Next**.

f At the *Select Computer* window, select **Local computer (the computer this console is running on)** and click **Finish**.

g Click **Close**.

h Click **OK**.

i In the *Console Root* folder, expand *Certificates (Local Computer)*.

j Go to the *Personal* folder and locate the desired certificate.

k Highlight the desired certificate, right-click **All Tasks > Export**.

l When the Certificate Export wizard opens, click **Next**.

m Select **Yes, export the private key** and click **Next**.

n Select **Personal Information Exchange - PKCS #12 (.PFX)** and then select the sub-options **Include all certificates in the certification path if possible** and **Export all extended properties**. Click **Next**.

o Enter and confirm a password. This can be any password of your choosing. Choose a password that is easy for you to remember, but no one else. Click **Next**.

p Click **Browse** to browse to the location of where you would like to save the file.

q In the *File Name* field, enter a name to save the file as. Click **Save**.

r Click **Next**.

s Click **Finish**.

t A message stating that the export was successful displays. Close the MMC.

u Go back to the Dell Server Configuration Tool.

v From the top menu, select **Actions > Import Manager Certificate**.

w Navigate to the location where the exported file was saved. Select the file and click **Open**.

x Enter the password associated with this file and click **OK**.

y From the top menu, select **Configuration > Save**. If prompted, confirm the save.

The Dell Manager certificate import is now complete.

9 Click the *Settings* tab.

Silverlight Console:

The default installation address of the Silverlight Console is automatically populated.

If your installation of Silverlight is hosted on a different server (such as a special IIS server), enter the address in the Silverlight Console URL field.

Manager:

To turn off Dell Manager SSL trust validation, check **Disable Trust Chain Check**.

NOTE: The client computer also must have the following registry entry to disable trust validation:

HKLM\System\CurrentControlSet\Services\CredMgmtAgent\Parameters\DisableSSLCertTrust (DWORD (32-bit) Value)=1

Disabling trust validation lessens security, but allows you to use a self-signed certificate for pilots, POCs, etc. For a production environment, Dell recommends public CA-signed or domain-signed certificates.

SCEP:

If using Dell Data Protection | Mobile Edition, enter the URL of the server hosting SCEP.

10 Click the *SMTP* tab.

This tab configures SMTP settings for Dell Data Protection | Cloud Edition. If SMTP settings need to be configured for other purposes outside of Dell Data Protection | Cloud Edition, see the AdminHelp topic "Enable SMTP Server for License Email Notifications".

Enter the following information:

a In the Host Name: field, enter the FQDN of your SMTP server, such as smtpservername.domain.com.

b In the User Name: field, enter the User Name that will log in to the mail server. The format can be DOMAIN\jdoe, jdoe, or whatever form your organization requires.

c In the Password: field, enter the Password associated with this User Name.

d In the From Address: field, enter the email address that the email will originate from. This may be the same as the account for the User Name (jdoe@domain.com), but it can also be another account that the specified User Name has access to send email for (CloudRegistration@domain.com).

e In the Port: field, enter the Port number (typically 25).

f In the Authentication: menu, select either True or False.

11 Finish configuration.

a From the top menu, select **Configuration > Save**. If prompted, confirm the save.

b Close the Dell Server Configuration Tool.

c Click **Start > Run**. Type *services.msc* and click **OK**. When *Services* opens, navigate to each Dell Service and click **Start the service**.

The Dell Server Configuration Tool logs to C:\Program Files\Dell\Enterprise Edition\Configuration Tool\Logs.

The rest of this chapter details the process for an upgrade/migration and may be ignored. Continue to Web Browser Version of Silverlight Console Configuration.

Configure a Migration

1 Launch the Dell Server Configuration Tool. Go to **Start > Programs > Dell > Enterprise Edition > Server Configuration Tool > Run Server Configuration Tool**.

2 You may get informational messages stating that your database configuration settings do not match. These messages are for information only and are not a cause for concern. If prompted, click **OK** for each message.

3 From the top menu, select **Configuration > Save**. If prompted, confirm the save.

4 Click the *Information* tab.

This tab is for information only and cannot be edited. All fields are pre-populated.

Core Server:	displays the installed location of the Dell Core Server.
Legacy Server:	displays the installed location of the Dell Compatibility Server.
Security Server:	displays the installed location of the Dell Security Server.
Messaging Service	displays the installed location of the Dell Messaging Service.
Compliance Reporter	displays the installed location of the Compliance Reporter.
Identity Server	displays the installed location of the Identity Server.
Schema Version:	displays the current database schema version.
Supported Versions:	displays the previous versions supported to migrate to the current version.

5 Click the *Database* tab.

a In the *Server Name:* field, enter the fully qualified domain name (if there is an instance name, include it) of the server hosting the database. For example, SQLTest.domain.com\DellDB.

Dell recommends using a fully qualified domain name, although an IP address may be used.

b In the *Database:* field, enter the name of the database.

c In the *Authentication:* field, select either **Windows Authentication** or **SQL Server Authentication**. If you choose Windows Authentication, the same credentials that were used to log in to Windows will be used for authentication (User Name and Password fields will not be editable).

d In the *User Name:* field, enter the appropriate username associated with this database.

e In the *Password:* field, enter the password for the username listed in the UserName field.

f From the top menu, select **Configuration > Save**. If prompted, confirm the save.

6 Test Database Configuration.

a From the top menu, select **Actions > Test Database Configuration**. The Configuration Wizard launches.

NOTE: The database cannot be migrated until after the database configuration tests have passed.

b At the *Configuration Test* window, read the test information and click **Next**.

c If you chose Windows Authentication in the *Database* tab, you can optionally enter alternate credentials to allow the use of the same credentials that will be used to run the Dell Enterprise Server. Click **Next**.

d At the *Test Configuration* window, the results of the Test Connection Settings, Compatibility Test, and the Database Migrated Test display.

You may get a failed test result for the Database Migrated Test, which is correct – this database has not been migrated yet. You cannot migrate this database until the two other tests, Test Connection Settings and Compatibility Test, have a result of Passed.

Click **Finish**.

e From the top menu, select **Configuration > Save**. If prompted, confirm the save.

7 Migrate Database.

a If you have not yet backed up your existing Dell database, **do so now**.

a From the top menu, select **Actions > Migrate Database**. The Configuration Wizard launches.

b At the *Migrate Enterprise Database* window, a warning displays. Confirm that you have either backed up the entire database or confirm that a backup does not need to be made of your existing database. Click **Next**.

c At the *Migrate Enterprise Database* window, read the information and click **Next**.

At the *Migrating Database* window, informational messages display the status of the migration.

When complete, check for errors.

NOTE: An error message identified by , signifies that a database task has failed and corrective action needs to be taken before the database can be properly migrated. Click Finish, correct the database errors, and reinitiate the instructions in this section.

d Click **Finish**.

e From the top menu, select **Configuration > Save**. If prompted, confirm the save.

8 Configure Certificates.

The first time you run the Dell Server Configuration Tool for initial Dell Enterprise Server setup, certificates must be configured for the Dell Compatibility Server, Dell Core Server, and Message Security.

You have a choice of which type of certificates to use – self-signed or signed:

– **Self-signed** certificates are signed by their own creator. Self-signed certificates are appropriate for pilots, POCs, etc. For a production environment, Dell recommends public CA-signed or domain-signed certificates.

– **Signed** (public CA-signed or domain-signed) certificates are signed by a public CA or a domain. In the case of certificates that are signed by a public certificate authority (CA), the certificate of the signing CA will, usually, already exist in the Microsoft certificate store and therefore, the chain of trust will be automatically established. For domain CA-signed certificates, if the workstation has been joined to the domain, the signing CA certificate from the domain will have been added to the workstation's Microsoft certificate store, thereby also creating a chain of trust.

The components that are affected by certificate configuration:

– Java Services (for instance, Dell Device Server, Dell Console Web Services, and so on)

– .NET Applications (Dell Core Server)

– Validation of smart cards used for Preboot Authentication (Dell Security Server)

– Importing of private encryption keys to be used for signing policy bundles being sent to Dell Manager. Dell Manager performs SSL validation for remotely-managed Enterprise Edition clients with Hardware Crypto Accelerators, self-encrypting drives, or BitLocker Manager.

– Client Workstations:

  · Workstations running the web browser version of the Silverlight Console

  · Workstations running Dell Data Protection | BitLocker Manager

  · Workstations running Dell Data Protection | Enterprise Edition (Windows clients)

Information regarding which type of certificates to use:

Preboot Authentication using smart cards requires SSL validation with the Dell Security Server. Dell Manager performs SSL validation when connecting to the Dell Core Server. The Silverlight Console also performs SSL validation. For these types of connections, the signing CA will need to be in the keystore (either the Java keystore or the Microsoft keystore, depending on which Dell Server component is being discussed). If self-signed certificates are chosen, the following options are available:

– Validation of smart cards used for Preboot Authentication:
  · Import the "Root Agency" signing certificate and full chain of trust into the Dell Security Server Java keystore. For more information, see Create a Self-Signed Certificate and Generate a Certificate Signing Request. The full chain of trust must be imported.
– Dell Manager:
  · Insert the "Root Agency" signing certificate (from the self-signed certificate generated) into the workstation's "Trusted Root Certification Authorities" (for "local computer") in the Microsoft keystore.
  · Modify the behavior of Dell Manager to not perform SSL validation. To turn off Dell Manager SSL trust validation, check **Disable Trust Chain Check** on the *Settings* tab.

  The client computer also must have the following registry entry to disable trust validation:

  HKLM\System\CurrentControlSet\Services\CredMgmtAgent\Parameters\DisableSSLCertTrust (DWORD (32-bit) Value)=1

  Disabling trust validation lessens security but allows you to use a self-signed certificate for pilots, POCs, etc. For a production environment, Dell recommends public CA-signed or domain-signed certificates.
– Workstations running the web browser version of the Silverlight Console:
  · Insert the "Root Agency" signing certificate (from Intermediate Certification Authorities) into the workstation's "Trusted Root Certification Authorities" (for "local computer") in the Microsoft keystore.

There are two methods to create a certificate – *Express* and *Advanced*.

Choose **one** method:

· Express – Choose this method to generate a self-signed certificate for all components. This is the easiest method.
· Advanced – Choose this method to configure each component separately.

Express

a From the top menu, select **Actions > Configure Certificates**.
b When the Configuration Wizard launches, select **Express** and click **Next**. The information from the self-signed certificate that was created when installing the Enterprise Server will be used, if available.
c From the top menu, select **Configuration > Save**. If prompted, confirm the save.

Certficate set up is complete. The rest of this section details the Advanced method of creating a certificate and may be ignored.

If your deployment includes Dell Manager, continue to step 9 on page 55.

If your deployment does **not** include Dell Manager, continue to step 10 on page 56.

Advanced

There are two paths to create a certificate – *Generate Self-Signed Certificate* and *Use Current Settings*.

Choose **one** path:

· Path 1 – Generate Self-Signed Certificate
· Path 2 – Use Current Settings

Path 1 – Generate Self-Signed Certificate

a From the top menu, select **Actions > Configure Certificates**.
b When the Configuration Wizard launches, select **Advanced** and click **Next**.
c Select **Generate Self-Signed Certificate** and click **Next**. The information from the self-signed certificate that was created when installing the Enterprise Server will be used, if available.
d From the top menu, select **Configuration > Save**. If prompted, confirm the save.

Certficate set up is complete. The rest of this section details the other method of creating a certificate and may be ignored.

If your deployment includes Dell Manager, continue to step 9 on page 55.

If your deployment does **not** include Dell Manager, continue to step 10 on page 56.

Path 2 – Use Current Settings

a From the top menu, select **Actions** > **Configure Certificates**.

b When the Configuration Wizard launches, select **Advanced** and click **Next**.

c Select **Use Current Settings** and click **Next**.

d At the *Compatibility Server SSL Certificate* window, select **Generate Self-Signed Certificate** and click **Next**. The information from the self-signed certificate that was created when installing the Enterprise Server will be used, if available.

Click **Next**.

e At the *Core Server SSL Certificate* window, select one of the following:

– *Select Certificate* – Select this option to use an existing certificate. Click **Next**.

Browse to the location of the existing certificate, enter the password associated with the existing certificate, and click **Next**.

Click **Finish** when complete.

– *Generate Self-Signed Certificate* – The information from the self-signed certificate that was created when installing the Enterprise Server will be used, if available. If you select this option, the Message Security Certificate window does not display (the window does display if you select option *Use Current Settings*) and the certificate created for the Dell Compatibility Server is used.

Verify that the fully qualified computer name is correct. Click **Next**.

A warning message displays, telling you that a certificate by the same name already exists. When asked if you would like to use it, click **Yes**.

Click **Finish** when complete.

– *Use Current Settings* – Select this option to change a setting on a certificate anytime after the initial configuration of the Dell Enterprise Server. Selecting this option leaves your already configured certificate in place. Selecting this option advances you to the Message Security Certificate window.

At the Message Security Certificate, select **one** of the following:

· *Select Certificate* – Select this option to use an existing certificate. Click **Next**.

Browse to the location of the existing certificate, enter the password associated with the existing certificate, and click **Next**.

Click **Finish** when complete.

· *Generate Self-Signed Certificate* – The information from the self-signed certificate that was created when installing the Enterprise Server will be used, if available.

Click **Next**.

Click **Finish** when complete.

f From the top menu, select **Configuration** > **Save**. If prompted, confirm the save.

Certficate set up is complete.

If your deployment includes Dell Manager, continue to step 9.

If your deployment does **not** include Dell Manager, continue to step 10.

9 Import Dell Manager Certificate.

If your deployment includes Enterprise Edition remotely-managed clients with Hardware Crypto Accelerators, self-encrypting drives, or BitLocker Manager, you must import your newly created (or existing) certificate. The Dell Manager certificate is used as a vehicle to protect the private key which is used to sign the policy bundles being sent to Enterprise Edition remotely-managed clients and BitLocker Manager. This certificate can be independent of any of the other certificates. Additionally, if this key is compromised it can be replaced with a new key, and Dell Manager will request a new public key if it cannot decrypt the policy bundles.

a Open the Microsoft Management Console.

b Click **File > Add/Remove Snap-in**.

c Click **Add**.

d At the *Add Standalone Snap-in* window, select **Certificates** and click **Add**.

e Select **Computer Account** and click **Next**.

f At the *Select Computer* window, select **Local computer (the computer this console is running on)** and click **Finish**.

g Click **Close**.

h Click **OK**.

i In the *Console Root* folder, expand *Certificates (Local Computer)*.

j Go to the *Personal* folder and locate the desired certificate.

k Highlight the desired certificate, right-click **All Tasks > Export**.

l When the Certificate Export wizard opens, click **Next**.

m Select **Yes, export the private key** and click **Next**.

n Select **Personal Information Exchange - PKCS #12 (.PFX)** and then select the sub-options **Include all certificates in the certification path if possible** and **Export all extended properties**. Click **Next**.

o Enter and confirm a password. This can be any password of your choosing. Choose a password that is easy for you to remember, but no one else. Click **Next**.

p Click **Browse** to browse to the location of where you would like to save the file.

q In the *File Name* field, enter a name to save the file as. Click **Save**.

r Click **Next**.

s Click **Finish**.

t A message stating that the export was successful displays. Close the MMC.

u Go back to the Dell Server Configuration Tool.

v From the top menu, select **Actions > Import Manager Certificate**.

w Navigate to the location where the exported file was saved. Select the file and click **Open**.

x Enter the password associated with this file and click **OK**.

y From the top menu, select **Configuration > Save**. If prompted, confirm the save.

The Dell Manager certificate import is now complete.

10 Click the *Settings* tab.

Silverlight Console:

The default installation address of the Silverlight Console is automatically populated.

If your installation of Silverlight is hosted on a different server (such as a special IIS server), enter the address in the Silverlight Console URL field.

Manager:

To turn off Dell Manager SSL trust validation, check **Disable Trust Chain Check**.

NOTE: The client computer also must have the following registry entry to disable trust validation:

HKLM\System\CurrentControlSet\Services\CredMgmtAgent\Parameters\DisableSSLCertTrust (DWORD (32-bit) Value)=1

Disabling trust validation lessens security, but allows you to use a self-signed certificate for pilots, POCs, etc. For a production environment, Dell recommends public CA-signed or domain-signed certificates.

SCEP:

If using Dell Data Protection | Mobile Edition, enter the URL of the server hosting SCEP.

11 Click the *SMTP* tab.

This tab configures SMTP settings for Dell Data Protection | Cloud Edition. If SMTP settings need to be configured for other purposes outside of Dell Data Protection | Cloud Edition, see the AdminHelp topic "Enable SMTP Server for License Email Notifications".

Enter the following information:

a In the Host Name: field, enter the FQDN of your SMTP server, such as smtpservername.domain.com.

b In the User Name: field, enter the User Name that will log in to the mail server. The format can be DOMAIN\jdoe, jdoe, or whatever form your organization requires.

c In the Password: field, enter the Password associated with this User Name.

d In the From Address: field, enter the email address that the email will originate from. This may be the same as the account for the User Name (jdoe@domain.com), but it can also be another account that the specified User Name has access to send email for (CloudRegistration@domain.com).

e In the Port: field, enter the Port number (typically 25).

f In the Authentication: menu, select either True or False.

12 Finish configuration.

a From the top menu, select **Configuration > Save**. If prompted, confirm the save.

b Close the Dell Server Configuration Tool.

c Click **Start > Run**. Type *services.msc* and click **OK**. When *Services* opens, click **Start the service**. for the Dell Message Broker, then the Dell Security Server. The remaining Services can be started in any order.

d As a Dell Administrator, log in to the Dell Remote Management Console.

e Click **Actions > Commit Policies**.

f Click **Apply Changes**.

g Log off the Dell Remote Management Console.

The Dell Server Configuration Tool logs to C:\Program Files\Dell\Enterprise Edition\Configuration Tool\Logs.

Configuration of the upgrade/migration is complete. Continue to Web Browser Version of Silverlight Console Configuration.

6

Web Browser Version of Silverlight Console Configuration

Complete the steps in this chapter if you intend to use the web browser version of the Silverlight Console. If not, continue to Administrative Tasks.

Add MIME Types

IIS 6 (Windows Server 2003)

Add the following MIME types. These MIME types may have already been added to IIS at some point. If so, continue to the next section once you verify that they are all present.

1. Open IIS Manager.
2. Expand the *Websites* folder.
3. Right-click **Default Website**.
4. Select **Properties**.
5. Select the *HTTP Headers* tab.
6. Click **MIME Types.**
7. Ensure that the following MIME types are present. If not, click **New** and follow the instructions below.
   - In the *Extension*: field, enter **.manifest**
   - In the *MIME types*: field, enter **application/manifest**
   - Click **OK**.

   - In the *Extension:* field, enter **.xaml**
   - In the *MIME types:* field, enter **application/xaml+xml**
   - Click **OK**.

   - In the *Extension:* field, enter **.xap**
   - In the *MIME types:* field, enter **application/x-silverlight-app**
   - Click **OK**.

   - In the *Extension:* field, enter **.dll**
   - In the *MIME types:* field, enter **application/x-msdownload**
   - Click **OK**.

   - In the *Extension:* field, enter **.application**
   - In the *MIME types:* field, enter **application/x-ms-application**
   - Click **OK**.

   - In the *Extension:* field, enter **.xbap**

- In the *MIME types:* field, enter **application/x-ms-xbap**
- Click **OK**.

- In the *Extension:* field, enter **.deploy**
- In the *MIME types:* field, enter **application/octet-stream**
- Click **OK**.

- In the *Extension:* field, enter **.xps**
- In the *MIME types:* field, enter **application/vnd.ms-xpsdocument**
- Click **OK**.

8 Click **OK** to apply the change.

IIS 7 (Windows Server 2008 and Windows Server 2008 R2)

These MIME types are pre-configured in IIS 7 (Windows Server 2008 and Windows Server 2008 R2). No action is needed.

IIS 8.5 (Windows Server 2012 R2)

These MIME types are pre-configured in IIS 8.5 (Windows Server 2012 R2). No action is needed.

Add Documents

IIS 6 (Windows Server 2003)

Add the following document type. This document type may have already been added to IIS at some point. If so, continue to the next section once you verify that it is present.

1 If needed, open IIS Manager.
2 Expand the *Websites* folder.
3 Expand *Default Website*.
4 Right-click **Console**.
5 Select **Properties**.
6 Select the *Documents* tab.
7 Ensure the checkbox *Enable default content page* is selected.
8 Ensure that **Default.aspx** is present. If not, click **Add** and follow the instructions below.
In the *Default content page*: field, enter **Default.aspx**
Click **OK**.
Highlight **Default.aspx** and click **Move Up** to move it to the top of the list.
9 Click **OK** to apply the change.

IIS 7 (Windows Server 2008 and Windows Server 2008 R2)

This document type is pre-configured in IIS 7 (Windows Server 2008 and Windows Server 2008 R2). No action is needed.

IIS 8.5 (Windows Server 2012 R2)

This document type is pre-configured in IIS 8.5 (Windows Server 2012 R2). No action is needed.

Enable ASP.NET 4.x

IIS 6 (Windows Server 2003)

1 If needed, open IIS Manager.
2 Expand the *Websites* folder.
3 Right-click **Default Website**.
4 Select **Properties**.
5 Select the *ASP.NET* tab.
6 In the *ASP.NET* version field, select 4.0.<xxxxx>.
7 Click **OK**.

IIS 7 (Windows Server 2008 and Windows Server 2008 R2)

1 Open a command prompt from C:\Windows\Microsoft.NET\Framework (or Framework64)\v4.0.30319.
2 Type the following command:
```
aspnet_regiis.exe -i
```

See http://msdn.microsoft.com/en-us/library/k6h9cz8h.aspx for additional information.

IIS 8.5 (Windows Server 2012 R2)

1 Open a command prompt from C:\Windows\Microsoft.NET\Framework64\v4.x.xxxxx.
2 Type the following command:
```
aspnet_regiis.exe -i
```

See http://msdn.microsoft.com/en-us/library/k6h9cz8h.aspx for additional information.

Convert Console to Application

IIS 6 (Windows Server 2003)

1 If needed, open IIS Manager.
2 Expand the *Websites* folder.
3 Expand *Default Website*.
4 Right-click **Console**.
5 Select **Properties**.
6 Select the *Directory* tab.
7 In the Application settings area, click **Create**.
The application is now created.
8 Select the *ASP.NET* tab. Ensure that ASP.NET version 4.0.<xxxxx> is selected.
9 Click **OK**.

IIS 7 (Windows Server 2008 and Windows Server 2008 R2)

1 If needed, open IIS Manager.
2 Expand the *Websites* folder.
3 Expand *Default Website*.
4 Right-click **Console**; select **Convert to Application**.
5 In the Application Pool area, ensure that *ASP.NET v4.0* is selected (not ASP.NET v4.0 Classic).
6 Click **OK**.
7 Close IIS Manager.

IIS 8.5 (Windows Server 2012 R2)

1 If needed, open IIS Manager.
2 Expand the *Websites* folder.
3 Expand *Default Website*.
4 Right-click **Console**; select **Convert to Application**.
5 In the Application Pool area, ensure that *ASP.NET v4.5* is selected.
6 Click **OK**.
7 Close IIS Manager.

Configure Web Service Extensions

IIS 6 (Windows Server 2003)

1 If needed, open IIS Manager.
2 Open the *Web Service Extensions* folder.
3 Highlight *All Unknown ISAPI Extensions* and click **Allow**.
4 You may get a message asking if you want to allow all unknown ISAPI extensions. If so, click **Yes**.
5 Close IIS Manager.

IIS 7 (Windows Server 2008 and Windows Server 2008 R2)

ISAPI extensions are pre-configured in IIS 7 (Windows Server 2008 and Windows Server 2008 R2). No action is needed.

IIS 8.5 (Windows Server 2012 R2)

ISAPI extensions are pre-configured in IIS 8.5 (Windows Server 2012 R2). No action is needed.

Enable Static Content

IIS 6 (Windows Server 2003)

No action is needed.

IIS 7 (Windows Server 2008 and Windows Server 2008 R2)

1 Open Server Manager.
2 Highlight **Roles**.
3 In the Role Service area, click **Add Role Service**.
4 Select **Web Server IIS Support** and click **Next**.
5 A dialog may display, asking *"Add role services and features required for Web Server (IIS) support?"*. If so, click **Add Required Role Services**.
6 Under *Common HTTP Features*, select **Static Content** and click **Next**.
7 Click **Install**.

IIS 8.5 (Windows Server 2012 R2)

1 Open Server Manager.
2 Highlight **Roles**.
3 In the Role Service area, click **Add Role Service**.
4 Select **Web Server IIS Support** and click **Next**.
5 A dialog may display, asking *"Add role services and features required for Web Server (IIS) support?"*. If so, click **Add Required Role Services**.

6 Under *Common HTTP Features*, select **Static Content** and click **Next**.

7 Click **Install**.

Enable IIS Management Console

IIS 6 (Windows Server 2003)

No action is needed.

IIS 7 (Windows Server 2008 and Windows Server 2008 R2)

1 If needed, open Server Manager.

2 Highlight **Roles**.

3 In the Role Service area, click **Add Role Service**.

4 Select **Web Server IIS Support** and click **Next**.

5 A dialog may display, asking *"Add role services and features required for Web Server (IIS) support?"*. If so, click **Add Required Role Services**.

6 Under *Management Tools*, select **IIS Management Console** and click **Next**.

7 Click **Install**.

8 When finished, close Server Manager.

IIS 8.5 (Windows Server 2012 R2)

1 If needed, open Server Manager.

2 Highlight **Roles**.

3 In the Role Service area, click **Add Role Service**.

4 Select **Web Server IIS Support** and click **Next**.

5 A dialog may display, asking *"Add role services and features required for Web Server (IIS) support?"*. If so, click **Add Required Role Services**.

6 Under *Management Tools*, select **IIS Management Console** and click **Next**.

7 Click **Install**.

8 When finished, close Server Manager.

The configuration of the web browser version of the Silverlight Console is now complete.

Test Configuration

Follow the instructions below to test the configuration of the web browser version of the Silverlight Console.

1 Launch Internet Explorer.

2 In the address bar, type <http://servername.domainname.com/console>.

3 Log in with the default credentials of superadmin/changeit.

If you experience errors, see Troubleshooting. Otherwise, continue to Administrative Tasks.

7

Administrative Tasks

Assign Dell Administrator Role

1 In the left pane, click Protect & Manage > Domains.
2 Click the *Members* icon of the Domain you want to add a user to.
3 Click Add Users.
4 Enter a filter to search the User Name by Common Name, Universal Principal Name, or sAMAccountName. The wild card character is *.

A Common Name, Universal Principal Name, and sAMAccountName must be defined in the enterprise directory server for every user. If a user is a member of a Domain or Group but does not appear in the Domain or Group Members list in the Dell Remote Management Console, ensure that all three names are properly defined for the user in the enterprise directory server.

The query will automatically search by common name, then UPN, and then sAMAccount name, until a match is found.

5 Select users from the *Directory User List* to add to the Domain. Use <Shift><click> or <Ctrl><click> to select multiple users.
6 Click Add Selected.
7 Click the *Details* icon of the specified user.
8 On the top menu, select the *Admin* tab.
9 Select the administrative roles to add to this user.
10 Click Save.

Log in with Dell Administrator Role

1 Log out of the Dell Remote Management Console.
2 Log in to the Dell Remote Management Console and login with Domain user credentials.

Upload Client Access License

You received Client Access Licenses separately from the installation files, either at the initial purchase or later if you added additional Client Access Licenses.

1 In the left pane, click Home.
2 Expand the Settings area (if needed), and click Client Licenses.
3 Click Browse to locate the Client License file.
4 Click Upload License File.

Apply a Policy Template

If desired, you can apply a policy template to the enterprise level. If you want policies to be applied at levels below the Enterprise levels, modify the individual policies.

The Policy Administrator and Superadmin are the only roles which can work with Policy Templates. The default policy templates are read-only.

1 In the left pane, click Protect & Manage > Enterprise.

2 Click **Security Policies** on the top menu. Highlight the policy template to apply, and click **Save**.

3 Click **Actions** > **Commit Policies**.

4 Click **Apply Changes**.

Your Policy Template is now applied as specified.

NOTE: You can optionally override a policy template by clicking Override.

TIP: Suppose you applied a template at the Enterprise level, saved, and then committed it. As expected, the Save and Cancel buttons are now inactive.

Now you click another template, and *that* template displays as the Local policy value. When you come back to the template page listing, the Save and Cancel buttons have become active again and the Local values display as the unsaved/uncommitted template.

In this situation, it can be difficult to distinguish which template is applied. To reset/unset the latest *unsaved* and *uncommitted* template, simply ctrl+left mouse click on the highlighted template name (the template name that is not saved or committed) to bring the Local values back to the saved and committed level.

Commit Policies

To commit polices that have been modified and saved, follow these steps:

1 In the left pane, click **Actions** > **Commit Policies**.

2 Click **Apply Changes**.

Configure Dell Compliance Reporter

1 In the left pane, click **Monitor** > **Compliance Reporter**.

2 When Dell Compliance Reporter launches, log in using the default credentials of *superadmin/changeit*.

3 Two different authentication methods are supported. To configure, select either:

- SQL Authentication
- Windows Authentication

SQL Authentication

As of v8.1, the Data Source is pre-configured out-of -the-box. No configuration is needed. Use the steps below to change the Data Source, if needed.

1 To set the Data Source, on the top menu, click **Settings**. In the left menu, click **Data Source**.

2 Type the Username to log in to the Dell database.

3 Type the Password to log in to the Dell database.

4 Type the Hostname to log in to the Dell database.

5 Type the Database Name to log in to the Dell database.

6 Type the Max Idle connections allowed. The default is 2.

7 Type the Max Connections (active) allowed. The default is 10.

8 Type the Max Wait (maximum number of milliseconds to wait for a connection). -1 is indefinitely.

9 To verify the database URL and test the connectivity between the Dell Compliance Reporter and the Dell database, click **Test Connection**.

10 Click **Update**. To discard the information, click Cancel.

Administrative tasks are complete. The rest of this chapter discusses Windows Authentication and may be ignored if SQL Authentication is used for Dell Compliance Reporter.

If needed, continue to Troubleshooting, Create a Self-Signed Certificate and Generate a Certificate Signing Request, or How to Export a Certificate to .PFX Using the Certificate Management Console.

Windows Authentication

As of v8.1, the Data Source is pre-configured out-of -the-box. No configuration is needed. Use the steps below to change the Data Source, if needed.

1. Type the Username to log in to the Dell database.
2. Leave the password blank. When the domain user logs in, their password will be passed to the database.
3. Type the Hostname to log in to the Dell database.
4. Type the Database Name to log in to the Dell database.
5. Type the Max Idle connections allowed. The default is 2.
6. Type the Max Connections (active) allowed. The default is 10.
7. Type the Max Wait (maximum number of milliseconds to wait for a connection). -1 is indefinitely.
8. To verify the database URL and test the connectivity between the Dell Compliance Reporter and the Dell database, click **Test Connection**.
9. Click **Update**. To discard the information, click Cancel.

Administrative tasks are complete. **If needed**, continue to Troubleshooting, Create a Self-Signed Certificate and Generate a Certificate Signing Request, or How to Export a Certificate to .PFX Using the Certificate Management Console.

Perform Back-ups

For the purposes of Disaster Recovery, ensure the following locations are backed up weekly, with nightly differentials:

DDPE Enterprise Server

Back up the files in "<Drive>:\Program Files\Dell" on a regular basis. Weekly backups of this data are acceptable, since it should rarely change and can be manually reconfigured if needed. The most critical files store information necessary to connect to the database:

<Drive>:\Program Files\Dell\Enterprise Edition\Compatibility Server\conf\server_config.xml

<Drive>:\Program Files\Dell\Enterprise Edition\Compatibility Server\conf\secretKeyStore

SQL Server

Perform nightly full backups with transactional logging enabled.

For additional information on SQL Server best practices, please see SQL Server Best Practices.

8

Troubleshooting

Visit support.dell.com for the most up-to-date troubleshooting information.

Troubleshoot Web Browser Version of Silverlight Console

If the web browser version of the Silverlight Console does not display, follow the steps below.

1. Open an Internet Explorer Browser.
2. On the browser toolbar, select **Tools** > **Internet Options**.
3. From the *Security* tab, highlight **Trusted Sites**.
4. Click **Sites**.
5. In the *Add this website to the zone:* field, verify that your FQDN displays in the text box.

   If not, add your FQDN. The format is http://servername.domainname.com.

   Click **Add**.
6. Re-attempt to open the web browser version of the Silverlight Console. Type in the Silverlight Console URL.

   The format is http://servername.domainname.com/console
7. If the web browser version of the Silverlight Console is installed, you will be asked to enter your credentials to access the Dell Remote Management Console.

   If you have not installed Silverlight, you will receive a notification asking if you would like to install Silverlight. Click **Click now to install** and follow the prompts to complete the installation.
8. You may get a security alert warning that your security settings do not allow this file to be downloaded. If so, click **OK**.
9. On the browser toolbar, select **Tools** > **Internet Options**.
10. From the *Security* tab, at the bottom of the window, click **Custom level**.
11. Scroll to *File download* and select **Enable** and click **OK**.
12. Re-attempt to open the web browser version of the Silverlight Console. Type in the Silverlight Console URL.

    The format is http://servername.domainname.com/console
13. If you have not installed Silverlight, you will receive a notification asking if you would like to install Silverlight. Click **Click now to install** and follow the prompts to complete the installation.

    OR

    As a Dell Administrator, log in to the Dell Remote Management Console. The default credentials are superadmin/changeit.

Troubleshoot Silverlight Console Error "Unable to Access the User Admin Roles"

The "Unable to Access the User Admin Roles" error is an end-to-end check to attempt to retrieve/validate the roles from the database. Therefore, SSL errors, network errors, database errors, IIS configuration issues, an so forth can all result in this problem.

One method to troubleshoot this error is to insert the certificate used by the Dell Core Server for STS signing into the Microsoft Certificate Store in Local Computer\Trusted People\Certificates.

The Dell Core Server is attempting to validate the signed STS token by using a certificate in the Microsoft Certificate Store in Local Computer\Trusted People\Certificates. If the certificate does not exist there, then the signing certificate validation will fail.

Another method to troubleshoot this error is to ensure that there is not a mismatch between the Dell Enterprise Server FQDN and the certificates (by configuring certificates using a DNS alias instead of the FQDN). This mismatch can happen if you installed the Dell Enterprise Server using the FQDN, but configured certificates using a DNS alias.

To troubleshoot this issue, change the "web.config" file in c:\inetpub\wwwroot\Console to reflect the CN of the certificate, as follows:

For this example, change the Dell Enterprise Server name from the FQDN (server01.domain.com) to the DNS alias (server01).

Once finished, restart the World Wide Web Publishing Service.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
For more information on how to configure your ASP.NET application, please visit http://go.microsoft.com/fwlink/?LinkId=169433
-->
<configuration>
        <system.web>
                <compilation targetFramework="4.0" />
                <pages>
                    <namespaces>
                        <add namespace="Credant.Console.Resources" />
                    </namespaces>
                </pages>
        </system.web>
        <appSettings>
            <!-- Credant.Console Default Settings -->
            <add key="Login.UseWindowsAuth" value="False" lockItem="true" />
            <add key="Settings.PageSize" value="25" lockItem="true" />
            <add key="Settings.StartScreen" value="Home" lockItem="true" />
            <add key="Settings.Brand" value="Credant" />
            <add key="Help.Uri" value="Help/" />
            <add key="Help.DefaultDocument" value="get_started.htm" />

            <!-- Credant.Server Settings -->
            <add key="ServercoreHostname" value="server01.domain.com" "server01" />
            <add key="ServercorePort" value="8888" />
            <add key="ServerHostname" value="server01.domain.com" "server01" />
            <add key="ServerPort" value="9011" />

            <!-- Credant.ComplianceReporter Settings -->
            <add key="ReporterHost" value="server01.domain.com" "server01" />
            <add key="ReporterPort" value="8084" />
            <add key="ReporterSslRequired" value="true" />

            <!-- Credant.Authorization.Sts Settings -->
            <add key="StsHost" value="server01.domain.com" "server01" />
            <add key="StsPort" value="9000" />
            <add key="DisableSSLCertTrust" value="True" />
            <add key="MaxReceivedMessageSize" value="1500000" />
        </appSettings>
  <system.webServer>
    <defaultDocument>
      <files>
        <clear />
        <add value="Default.htm" />
        <add value="Default.asp" />
        <add value="default.aspx" />
        <add value="index.htm" />
        <add value="index.html" />
        <add value="iisstart.htm" />
      </files>
    </defaultDocument>
  </system.webServer>
</configuration>
```

A

Appendix A

Dell Component Descriptions

The following table describes each component and its function.

.

Name	Description	Required For
Dell Compliance Reporter	Provides an extensive view of the environment for auditing and compliance reporting. A component of the Dell Enterprise Server.	Reporting
Dell Key Server	A Service that negotiates, authenticates, and encrypts a client connection using Kerberos APIs. A component of the Dell Enterprise Server.	Dell Admin Utilities
Dell Server Configuration Tool	Configures database communication with the Dell Core Server and Dell Compatibility Server/Dell Security Server. Used to initialize the database upon installation or to migrate the database to a newer schema. Used to control Dell Services. A component of the Dell Enterprise Server.	All
Dell Remote Management Console	Administration console and control center for the entire enterprise deployment. A component of the Dell Enterprise Server.	All
Dell Console Web Services	Supports Dell Enterprise Server communication with the Dell Compatibility Server. A component of the Dell Enterprise Server.	All
Dell Core Server	Used for policy and license management as well as providing policy updates and registration for Dell Data Protection I SED Management and Dell Data Protection I BitLocker Manager. A component of the Dell Enterprise Server.	All
Silverlight Console	Web browser version of the administration console and control center for the entire enterprise deployment. A component of the Dell Enterprise Server.	Not required
Dell Security Server	Provides the mechanism for controlling commands and communication with AD. Used to communicate with the Dell Policy Proxy. A component of the Dell Enterprise Server.	All

Name	Description	Required For
Dell Compatibility Server	A Service for managing the enterprise architecture. A component of the Dell Enterprise Server.	All
Dell Message Broker Service	Handles communication between the services of the Dell Enterprise Server.	All
Dell Device Server	Supports activations and password recovery. A component of the Dell Enterprise Server.	Dell Data Protection | Enterprise Edition for Mac Dell Data Protection | Enterprise Edition for Windows CREDActivate
Dell Device Server Plug-ins	Provides support for various components. A component of the Dell Enterprise Server.	All
Dell Identity Server	Handles domain authentication requests. Requires an AD account. Must be the account used to access SQL when Windows Authentication is used. A component of the Dell Enterprise Server.	All
Dell Policy Proxy	Provides a network-based communication path to deliver security policy updates and inventory updates. A component of the Dell Enterprise Server.	Dell Data Protection | Enterprise Edition for Mac Dell Data Protection | Enterprise Edition for Windows Dell Data Protection | Mobile Edition
Security Token Services (STS)	Used to help create a secure authentication channel between the Dell Enterprise Server User Interface and Dell back-end Services.	All
EAS Device Manager	Enables over-the-air functionality. Installed on the Exchange Client Access Server.	Exchange ActiveSync Management of mobile devices.
EAS Mailbox Manager	The mailbox agent that is installed on the Exchange Mailbox Server.	Exchange ActiveSync Management of mobile devices.

B

Appendix B

SQL Server Best Practices

The following list explains SQL server best practices, which should be implemented when Dell Data Protection is installed if not already implemented.

1 Ensure the NTFS block size where the data file and log file reside is 64 KB. SQL Server extents (basic unit of SQL Storage) are 64 KB.

For more information, search Microsoft's TechNet articles for "Understanding Pages and Extents."

- Microsoft SQL Server 2008 - http://technet.microsoft.com/en-us/library/ms190969%28v=sql.100%29
- Microsoft SQL Server 2008 R2 - http://technet.microsoft.com/en-us/library/ms190969(v=sql.105).aspx

2 As a general guideline, set the maximum amount of SQL Server memory to 80 percent of the installed memory.

For more information, search Microsoft's TechNet articles for "Server Memory Server Configuration Options."

- Microsoft SQL Server 2008 - http://technet.microsoft.com/en-us/library/ms178067%28v=sql.100%29
- Microsoft SQL Server 2008 R2 - http://technet.microsoft.com/en-us/library/ms178067%28v=sql.105%29
- Microsoft SQL Server 2012 - http://technet.microsoft.com/en-us/library/ms178067%28v=sql.110%29

3 Set -t1222 on the instance startup properties to ensure deadlock information is captured if one occurs.

For more information, search Microsoft's TechNet articles for "Trace Flags (Transact-SQL)."

- Microsoft SQL Server 2008 - http://technet.microsoft.com/en-us/library/ms188396%28v=sql.100%29
- Microsoft SQL Server 2008 R2 - http://technet.microsoft.com/en-us/library/ms188396%28v=sql.105%29
- Microsoft SQL Server 2012 - http://technet.microsoft.com/en-us/library/ms188396%28v=sql.110%29

4 Ensure that all Indexes are covered by a weekly maintenance job to rebuild the indexes.

C

Appendix C

Certificates

Create a Self-Signed Certificate and Generate a Certificate Signing Request

This section details the steps to create a self-signed certificate for the Java-based components. This process **cannot** be used to create a self-signed certificate for .NET-based components.

We recommend a self-signed certificate *only* in a non-production environment.

If your organization requires an SSL server certificate, or you need to create a certificate for other reasons, this section describes the process to create a java keystore using Keytool.

If your organization plans to use smart cards for authentication, you will need to use Keytool to import the full certificate chain of trust that are used in the smart card user's certificate.

Keytool creates private keys that are passed in the format of a Certificate Signing Request (CSR) to a Certificate Authority (CA), such as VeriSign® or Entrust®. The CA will then, based on this CSR, create a server certificate that it signs. The server certificate is then downloaded to a file along with the signing authority certificate. The certificates are then imported into the cacerts file.

Generate a New Key Pair and a Self-Signed Certificate

1 Navigate to the **conf** directory of Dell Compliance Reporter, Dell Console Web Services, Dell Security Server, or Dell Device Server.

2 Back up the default certificate database:

Click **Start > Run**, and type **move cacerts cacerts.old**.

3 Add Keytool to the system path. Type the following command in a command prompt:

```
set path=%path%;<Dell Java Install Dir>\bin
```

4 To generate a certificate, run Keytool as shown:

```
keytool -genkey -keyalg RSA -sigalg SHA1withRSA -alias Dell -keystore .\cacerts
```

5 Enter the following information as the Keytool prompts for it.

NOTE: Back up configuration files before editing them. Only change the specified parameters. Changing other data in these files, including tags, can cause system corruption and failure. Dell cannot guarantee that problems resulting from unauthorized changes to these files can be solved without reinstalling the Dell Enterprise Server.

- *Keystore password*: Enter a password (unsupported characters are <>;&" '), and set the variable in the component **conf** file to the same value, as follows:

  <Compliance Reporter install dir>\conf\eserver.properties. Set the value eserver.keystore.password =

  <Console Web Services install dir>\conf\eserver.properties. Set the value eserver.keystore.password =

  <Device Server install dir>\conf\eserver.properties. Set the value eserver.keystore.password =

  <Security Server install dir>\conf\eserver.properties. Set the value eserver.keystore.password =

- *Fully Qualified Server Name*: Enter the fully qualified name of the server where the component you are working with is installed. This fully qualified name includes the host name and the domain name (example, server.domain.com).
- *Organizational unit*: Enter the appropriate value (example, Security).
- *Organization*: Enter the appropriate value (example, Dell).

- *City or locality*: Enter the appropriate value (example, Dallas).
- *State or province*: Enter the unabbreviated state or province name (example, Texas).
- Two-letter country code.
- The utility prompts for confirmation that the information is correct. If so, type `yes`.

If not, type `no`. The Keytool displays each value entered previously. Click **Enter** to accept the value or change the value and click **Enter**.

– *Key password for alias*: If you do not enter another password here, this password defaults to the Keystore password.

Request a Signed Certificate from a Certificate Authority

Use this procedure to generate a Certificate Signing Request (CSR) for the self-signed certificate created in Generate a New Key Pair and a Self-Signed Certificate.

1 Substitute the same value used previously for **<certificatealias>**:

```
keytool -certreq -sigalg SHA1withRSA -alias <certificate-alias> -keystore .\cacerts -file
<csr-filename>
```

For example, `keytool -certreq -sigalg SHA1withRSA -alias sslkey -keystore .\cacerts -file Dell.csr`

The .csr file will contain a BEGIN/END pair that will be used during the creation of the certificate on the CA.

2 Follow your organizational process for acquiring an SSL server certificate from a Certificate Authority. Send the contents of the <csr-filename> for signing.

NOTE: There are several methods to request a valid certificate. An example method is shown in Example Method to Request a Certificate.

3 When the signed certificate is received, store it in a file.

4 As a best practice, back up this certificate in case an error occurs during the import process. This backup will prevent having to start the process over.

Import a Root Certificate

If the root certificate Certificate Authority is Verisign (but not Verisign Test), skip to the next procedure and import the signed certificate.

The Certificate Authority root certificate validates signed certificates.

1 Do **one** of the following:

- Download the Certificate Authority root certificate, and store it in a file.
- Obtain the enterprise directory server root certificate.

2 Do **one** of the following:

- If you are enabling SSL for Dell Compliance Reporter, Dell Console Web Services, Dell Security Server, or Dell Device Server, change to the component **conf** directory.
- If you are enabling SSL between the Dell Enterprise Server and the enterprise directory server, change to **<Dell install dir>\Java Runtimes\jre1.x.x_xx\lib\security** (the default password for JRE cacerts is **changeit**).

3 Run Keytool as follows to install the root certificate:

```
keytool -import -trustcacerts -alias <ca-cert-alias> -keystore .\cacerts -file
<ca-cert-filename>
```

For example, `keytool -import -alias Entrust -keystore .\cacerts -file .\Entrust.cer`

Example Method to Request a Certificate

An example method to request a certificate is to use a web browser to access the Microsoft CA Server, which will be set up internally by your organization.

1 Navigate to the Microsoft CA Server. The IP address will be supplied by your organization.

2 Select **Request a certificate** and click **Next**.

3 Select **Advanced Request** and click **Next**.

4 Select the option to **Submit a certificate request using a base64 encode PKCS #10 file** and click **Next**.

5 Paste in the contents of the CSR request in the text box. Select a certificate template of **Web Server** and click **Submit**.

6 Save the certificate. Select **DER encoded** and click **Download CA certificate**.

7 Save the certificate. Select **DER encoded** and click **Download CA certification path**.

8 Import the converted signing authority certificate. Return to the DOS window. Type:

```
keytool -import -trustcacerts -file <csr-filename> -keystore cacerts
```

9 Now that the signing authority certificate has been imported, the server certificate can be imported (the chain of trust can be established). Type:

```
keytool -import -alias sslkey -file <csr-filename> -keystore cacerts
```

Use the alias of the self-signed certificate to pair the CSR request with the server certificate.

10 A listing of the cacerts file will show that the server certificate has a **certificate chain length** of **2**, which indicates that the certificate is not self-signed. Type:

```
keytool -list -v -keystore cacerts
```

The certificate fingerprint of the second certificate in the chain is the imported signing authority certificate (which is also listed below the server certificate in the listing).

The server certificate has successfully been imported, along with the signing authority certificate.

How to Export a Certificate to .PFX Using the Certificate Management Console

Once you have a certificate in the form of a .crt file in the MMC, it must be converted to a .pfx file for use with Keytool when the Dell Security Server is used in DMZ Mode *and* when importing a Dell Manager certificate into the Dell Server Configuration Tool.

1 Open the Microsoft Management Console.

2 Click **File > Add/Remove Snap-in**.

3 Click **Add**.

4 At the *Add Standalone Snap-in* window, select **Certificates** and click **Add**.

5 Select **Computer Account** and click **Next**.

6 At the *Select Computer* window, select **Local computer (the computer this console is running on)** and click **Finish**.

7 Click **Close**.

8 Click **OK**.

9 In the *Console Root* folder, expand *Certificates (Local Computer)*.

10 Go to the *Personal* folder and locate the desired certificate.

11 Highlight the desired certificate, right-click **All Tasks > Export**.

12 When the Certificate Export wizard opens, click **Next**.

13 Select **Yes, export the private key** and click **Next**.

14 Select **Personal Information Exchange - PKCS #12 (.PFX)** and then select the sub-options **Include all certificates in the certification path if possible** and **Export all extended properties**. Click **Next**.

15 Enter and confirm a password. This can be any password of your choosing. Choose a password that is easy for you to remember, but no one else. Click **Next**.

16 Click **Browse** to browse to the location of where you would like to save the file.

17 In the *File Name* field, enter a name to save the file as. Click **Save**.

18 Click **Next**.

19 Click **Finish**.

A message stating that the export was successful displays. Close the MMC.

How to Add a Trusted Signing Cert to the Security Server when an Untrusted Certificate was used for SSL

1 Stop the Security Server Service, if running.

2 Back up the cacerts file in <Security Server install dir>\conf\.

Use Keytool to complete the following:

3 Export the trusted PFX into a text file and document the Alias:

```
keytool -list -v -keystore "C:\pfxfilename.pfx" -storetype PKCS12 >C:\pfxfilename.txt
```

4 Import the PFX into the cacerts file in <Security Server install dir>\conf\.

```
keytool -importkeystore -v -srckeystore "C:\pfxfilename.pfx" -srcstoretype PKCS12
-srcalias AliasNamePreviouslyDocumented -destkeystore "C:\Program Files\Dell\Enterprise
Edition\Security Server\conf\cacerts" -deststorepass changeit  -destalias
AliasNamePreviouslyDocumented -destkeypass changeit
```

5 Modify the keystore.alias.signing value in <Security Server install dir>\conf\application.properties.

```
keystore.alias.signing=AliasNamePreviouslyDocumented
```

6 Start the Security Server Service.

0 XXXXXA0 X